IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

IN RE EQUIFAX, INC. DERIVATIVE LITIGATION	CIVIL ACTION FILE NO. 1:18-CV-317-TWT

VERIFIED CONSOLIDATED SHAREHOLDER DERIVATIVE COMPLAINT

WEISSLAW LLP
Joseph H. Weiss
David C. Katz
Mark D. Smilow
Joshua M. Rubin
1500 Broadway, 16th Floor
New York, New York 10036

Michael A. Rogovin
476 Hardendorf Ave. NE
Atlanta, Georgia 30307

Counsel for Lead Plaintiffs
Nancy A.K. and John Weyl and
Lead Derivative Counsel

TABLE OF CONTENTS

Lead Plaintiffs Nancy A.K. and John Weyl, derivatively on behalf of Nominal Defendant Equifax, Inc. ("Equifax" or the "Company"), for their Verified Consolidated Shareholder Derivative Complaint against defendants, allege the following upon personal knowledge as to themselves and their own acts, and upon information and belief as to all other matters, based upon the investigation conducted by Court appointed Lead Counsel. This investigation included, among other things, a review of the Company's announcements and press releases, filings made by the Company with the United States Securities and Exchange Commission ("SEC"), corporate governance documents available on the Company's website, governmental and regulatory investigations of the Company and testimony and documents relating thereto, research reports by securities analysts, analyses by and consultation with cybersecurity experts, transcripts of Equifax investor conference calls, news reports and other publicly available information about the Company.

I. PRELIMINARY STATEMENT

1. This derivative litigation arises out of the Individual Defendants', as defined in detail at ¶¶ 41 - 57, below, egregious and extensive breaches of fiduciary duties; failures of risk oversight, information security, internal control monitoring, crisis management, governance, and disclosure controls; non-

compliance with applicable laws, regulations, industry standards and Equifax's Code of Ethics and Business Conduct; and utter disregard for safeguarding the critically sensitive and confidential information and data which they undertook to guard and which is the core of Equifax's business.

2. Equifax provides information solutions and human resources business process outsourcing services for businesses, governments, and consumers, based on its comprehensive databases of consumer and business information derived from numerous sources. The Company operates through four segments: U.S. Information Solutions ("USIS"), International, Workforce Solutions, and Global Consumer Solutions. Equifax serves customers in financial service, mortgage, human resource, consumer, commercial, telecommunication, retail, automotive, utility, brokerage, healthcare, and insurance industries, as well as state and federal governments. As part of Equifax's business, it obtains and stores highly sensitive and private information concerning almost half of all United States citizens and numerous foreign nationals.

3. The breaches of duties involved herein resulted in the largest and most costly data breach (the "Data Breach" or "Breach") in corporate history, exposing more than half of the adult population of the United States to identity theft and subjecting Equifax to material enterprise risk from enormous liability, damages,

penalties and fines in securities, consumer and financial institution class action litigation; numerous other lawsuits and civil enforcement actions by states, cities, and others; investigations by the SEC, the Department of Justice (the "DOJ"), the Federal Trade Commission (the "FTC"), the Consumer Financial Protection Bureau ("CFPB"), the Financial Industry Regulatory Authority ("FINRA"), state banking regulators, congressional committees in both the United States Senate and House of Representatives, 49 state Attorneys General, and British and Canadian governmental authorities; lost business and cancelled contracts; resource constraints; incremental IT and data security costs; legal, consulting, investigative, and other fees and expenses; severe and lasting damage to the Company's brand, reputation, and competitive position; and the loss of billions of dollars of market capitalization.

4. Equifax has conceded the cause of the Data Breach. In March 2017, Equifax was expressly warned that one of its key software applications suffered from a material vulnerability. Equifax was warned by numerous sources that it urgently needed to install a patch on the software by performing a simple upgrade. However, Equifax did not install the upgrade. Two months later, hackers infiltrated Equifax's systems and, over several weeks, stole the most highly sensitive Personal Identity Information ("PII") pertaining to 145.5 million

individuals, or approximately 57.5% of the Country's adult population. Despite repeated warnings of the critical security vulnerability since at least March 2017, Equifax did not discover the Data Breach until the last days of July, and it did not inform the public about the Data Breach until mid-September.

5. Equifax's response to the Data Breach was wholly inadequate. Instead of giving prompt notice to victims and offering adequate data theft security protection, Equifax directed its victims to Equifax's own poorly designed website. Victims were unable to obtain necessary information and calls to the telephone hotline were dropped or resulted in excruciatingly long waits. To compound their wrongful acts, and further jeopardize the Company's reputation and credibility, Equifax then undertook to sell its own data protection plans to its victims. Instead of remunerating the victims of their faithless conduct, the Individual Defendants sought to profit from the Data Breach.

6. The Data Breach, by far the most severe in American history, was the result of a critical vulnerability in the Apache Struts software, an open-source web application framework used to develop Java web applications. The vulnerability was first reported by security firms and in online security bulletins by the Apache Software Foundation, the Apache Struts developer, on March 7, 2017. The security announcement urgently warned that the software was vulnerable to

"Remote Code Execution," allowing hackers to penetrate website servers. The warning ranked the vulnerability as "critical," the "maximum security rating."

7. The alert was emailed to Equifax the following day by the United States Department of Homeland Security, Computer Emergency Readiness Team, which designated the severity of the vulnerability as "high" and expressly instructed Equifax to implement the patch.

8. On March 10, 2017, the Department of Commerce, National Institute of Standards and Technology, provided notice of the vulnerability in its National Vulnerability Database, scoring the vulnerability as a 10, the highest possible score.

9. The critical vulnerability and the need to address it immediately were also widely reported in computer and technology professional publications, with headlines such as that in *The Register*: "Apache Struts 2 Needs Patching Now, Without Delay. It's Under Attack Now." With open source software like the Apache Struts, the responsibility to download and load patches rests with the user. The instructions for doing so and remedying the problem were clear and simple.

10. Although Equifax conducted two scans of its systems for Apache Struts vulnerabilities on or about March 9 and 15, 2017, it came up empty handed because its scanners were outdated. As one expert, Pravin Kothari, CEO of

CipherCloud, has noted, Equifax had a "weak and broken" security process. "A good security process would have identified vulnerable systems within 24 hours," he said.

11. The patch was not installed and no one at Equifax, not its officers, not its directors, not the members of the Audit Committee, not the members of the Technology Committee, and not its Chief Information and Security Officer, even bothered to inquire whether it was installed.

12. On May 13, 2017, more than two months after the patch was available and the alerts and instructions were provided to Equifax, which could have promptly and easily remedied the critical vulnerability, hackers began exploiting the patch-less system's glaring weaknesses, easily accessing and stealing millions of files containing user names and passwords, with which they then hacked the Company's internal systems until Equifax belatedly noticed suspicious network traffic more than two and a half months later, on July 29, 2017. The hackers retrieved the highly confidential, unencrypted personal information of 148 million Americans and almost one million Britons and Canadians, including names, addresses, Social Security numbers, passport numbers and photos, birth dates, driver license information and tax identification numbers, "the crown jewels of personal information." The hackers hit the Mother Lode.

13. On August 2, 2017, five months after being warned and instructed to install the patch, Equifax notified the Federal Bureau of Investigation (the "FBI") that hackers had gained "criminal access" to its computer network and stole staggering amounts of personal information in the euphemistically called "cybersecurity incident." The Equifax Board of Directors was notified of the Breach not more than three weeks later, on August 24, 2017, and met for the first time to discuss the matter a week later, on September 1, 2017.

14. Public disclosure of the Breach was not made until September 7, 2017, almost four months after it occurred, five weeks after it became known to the Company and at least two weeks after it became known to the Company's directors. The extensive delay meant that the millions of people affected by the Breach had not taken steps to protect themselves. As the *Atlanta Journal-Constitution* reported in a December 29, 2017 article: "The news immediately sent a shudder through the financial world."

15. Prior to making the delayed public disclosure of the Data Breach, several Equifax executives quickly acted to line their own pockets before the harm to the Company was publicly revealed. On August 1-2, 2017, a day after Equifax discovered the Data Breach, but well before disclosure, defendants John W. Gamble, Chief Financial Officer ("CFO") ("Gamble"), Joseph M. ("Trey")

Loughran, III, President, U.S. Information Solutions ("Loughran"); Rodolfo O. ("Rudy") Ploder, President, Workforce Solutions ("Ploder"); and Douglas Brandberg, Senior Vice President, Investor Relations ("Brandberg") sold Equifax shares valued at nearly $2 million. The DOJ and the SEC are investigating the sales. To date, two Equifax employees have been indicted on insider trading charges. One has pled guilty.

16. On September 14, 2017, *Wired* published an article titled "Equifax Officially Has No Excuse," in which it said:

> Capping a week of incompetence, failures, and general shady behavior in responding to its data breach, Equifax has confirmed that attackers entered its system in mid-May through a web-application vulnerability that had a patch available in March. In other words, the credit-reporting giant had more than two months to take precautions that would have defended the personal data of 143 million people from being exposed. It didn't.
>
> As the security community processes the news and scrutinizes Equifax's cybersecurity posture, numerous doubts have surfaced about the organization's competence as a data steward. The company took six weeks to notify the public after finding out the breach. Even then, the site that Equifax set up in response to address questions and offer free credit monitoring was itself riddled with vulnerabilities . . . the ongoing discoveries increasingly paint a picture of negligence – especially in Equifax's failure to protect itself against a known flaw with a ready fix.

17. On April 11, 2018, CtW Investment Group ("CtW"), an investment management firm which also provides proxy analysis and guidance to pension

funds and others, issued a report (the "CtW Report") urging that shareholders vote at Equifax's Annual Meeting on May 3, 2018 against the reelection of defendants John A. McKinley ("McKinley"), Mark B. Templeton ("Templeton") and Mark L. Feidler ("Feidler") as Board members. The CtW Report noted that these three directors were long-term members of the Technology Committee of the Board and that McKinley also served as a long-term member of the Audit Committee of the Board, notwithstanding that, according to a 2017 Equifax Board Skills Matrix, he lacked "risk management" experience. CtW explained that the directors "failed to provide timely and adequate risk oversight over a material enterprise risk despite numerous warnings;" they "failed to develop a comprehensive crisis management plan in the wake of the breach, which further damaged the company's reputation;" and "McKinley, as a member of the Audit Committee, failed to provide adequate risk oversight of the company's legal and compliance obligations."

18. CtW also noted that "index provider MSCI had warned Equifax almost a year before the Data Breach was disclosed that Equifax was not equipped to respond to a data breach, finding no evidence that the Company conducted regular cybersecurity audits or that it had adequate response plans in place." Moreover, "both the Audit Committee and the Technology Committee were empowered with the tools necessary to identify and possibly even avoid the

massive data breach that took place, but failed to execute the responsibilities and duties required of them."

19. On April 26, 2018, Institutional Shareholder Services Inc. ("ISS"), a leading provider of proxy and governance analysis and vote recommendations, issued a report (the "ISS Report") urging that shareholders vote against the reelection of defendants McKinley, Templeton, Feidler, G. Thomas Hough ("Hough") (a member of the Technology and Audit Committees), and Elane B. Stock ("Stock") (a member of the Technology Committee) as Board members, "as the severity of the cybersecurity breach and the company's slow response to it damaged the company's reputation, destroyed shareholder value and placed a cloud over the company for the foreseeable future." The ISS Report added that "it is certain that the full impact of the breach has not yet been felt. . . . the degree to which criminals make use of data stolen from Equifax . . . may not be apparent for months or even years."

20. ISS Report further noted that:

> The cybersecurity incident experienced by the company in 2017 has had a significant impact on shareholders already, and will likely continue to have an impact in coming years. In light of the enormous amounts of sensitive consumer data held by the company, as well as the occurrence of high-profile data breaches at numerous other companies in recent years, Equifax was clearly a likely target for cyberattacks, and it needed to have not only robust defense measures,

> but a robust crisis plan as well. It was entirely foreseeable that a failure by the company to protect consumer information would result in litigation, regulatory action and a loss of business, not to mention severe damage to the company brand and a loss of shareholder value. For a company whose business is based on the commercial use of personal information, that is generally not provided to it directly by the persons themselves, protecting that information, and maintaining a societal license to continue to collect and use it, is arguably one of the board's most important responsibilities.

21. On April 10, 2018, Merrill Lynch initiated coverage of Equifax with an Underperform rating, stating: "In our view, the 2017 data breach will lead to material one-time costs, lasting damage to its US consumer-facing business, legal settlements, potential legislative/regulatory changes, and possible market share losses. We view Equifax's brand as impaired."

22. Moreover, these failures and the Company's slow and bungled response to the Data Breach, took place notwithstanding the Individual Defendants' knowledge that:

(i) As a "global data-analytics company," credit data is the "core" of the Company's business and strong data security – indeed, "heightened security" and hyper-vigilance – is critical to its operations and profitability;

(ii) Cyber-crime is one of the world's fastest growing and most lucrative industries and cyber-attacks are one of the greatest risks to financial institutions, including Equifax;

(iii) Equifax had previously been hacked numerous times and its vast "information bank" makes it a prime target of criminals seeking to obtain the massive amounts of personal identity information located in its computers;

(iv) Equifax has a cybersecurity "Most Inherent Risk Profile" as defined by the Federal Financial Institutions Examination Council, which is comprised of the principals of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau and State Liaison Committee;

(v) Equifax had represented publicly that safeguarding the security and confidentiality of the information in its network, its primary asset, is a "top priority" for the Company, and that the Company maintains a "rigorous" enterprise risk and crisis management program, "advanced security, protections and redundancies" and takes every precaution to ensure security;

(vi) The Company's consultants, cybersecurity experts, and an investment research firm had repeatedly warned the Individual Defendants that, contrary to their representations, Equifax's data security practices, policies and standard of care were materially deficient and its systems were

highly vulnerable to attack; it was not equipped to respond to a data breach – to the contrary, it had outdated and ineffective cybersecurity protections and misconfigured security policies; it urgently needed to update and patch obsolete and outdated software, to implement and maintain adequate encryption and authentication measures, to put in place more effective fraud monitoring and scanning of its computer networks and systems, to develop and maintain a comprehensive data breach plan, to conduct regular cybersecurity audits, to provide training to employees in identifying risks, and to take other remedial actions;

(vii) The accounting and consulting firm hired to perform a security audit in 2016 warned Equifax that its approach to patching systems was "careless";

(viii) The developer of the software used by Equifax warned of the software's vulnerability to hacking and, accordingly, made available a "patch" which was described in news articles, government alerts, and industry notices as "critical" to addressing security weaknesses;

(ix) The United States Department of Homeland Security issued an alert and emailed Equifax directly, instructing it to install the "patch";

(x) The Department of Commerce issued a similar alert regarding the necessity of installing the "patch"; and

(xi) As Equifax and the Individual Defendants represented in the Company's Annual Reports and other public filings, a data breach "could subject us to litigation, regulatory fines, penalties or reputational damage, any of which could have a material effect on our cash flows, competitive position, financial condition or results of operations" and the potential liability, damages and expenses in the event of a massive hack were so great that the very survival of Equifax could be imperiled. As *Bloomberg Business Week* reported in its September 29, 2017 edition, "In the corridors and break rooms of Equifax Inc.'s giant Atlanta headquarters, employees used to joke that their enormously successful credit reporting company was just one hack away from bankruptcy."

23. Nevertheless, the Individual Defendants failed to take the necessary steps to implement and maintain effective controls over data security and simply ignored the alerts, warnings and instructions of the software developer, the Company's own consultants, government and industry experts, and the Departments of Homeland Security and Commerce, and did not update its

software, install the patch or take other necessary and appropriate required steps to ensure data security.

24. Moreover, although Equifax's Code of Ethics and Business Conduct explicitly warns that each of the officers and directors "must be vigilant and protect confidential information," none of them even inquired whether the software had been updated, whether the patch had been applied or whether other material actions had been taken.

25. Richard F. Smith ("Smith"), the former Chairman and Chief Executive Officer of Equifax admitted: "We at Equifax clearly understood that the collection of American consumer information and data carries with it enormous responsibility to protect that data. We did not live up to that responsibility."

26. Indeed, Equifax's officers and directors consciously failed to act in the face of a known duty to protect the confidential data entrusted to the Company and merely paid lip service to maintaining data security. Contrary to the representation in Equifax's 2017 Proxy Statement, under the heading "Board Expertise and Skills," that "Our Board is composed of experienced leaders with the right skill and business experience to provide sound judgment, critical viewpoints and guidance," the members of the Board's Technology Committee, whose responsibilities include providing "guidance on technology as it may pertain to,

among other things, . . . security concerns" and overseeing "the execution of technology strategies formulated by management and technology risks," did not have data risk management expertise or experience or "the right skill and business experience to provide sound judgment, critical viewpoints and guidance."

27. Moreover, Equifax's Chief Information Security Officer ("CISO"), Susan Mauldin, who was in charge of protecting against and combatting cybersecurity threats, had no formal training in information systems, cybersecurity, or technology; her credentials were a Master of Fine Arts degree in music composition. While that may not have been the cause of the catastrophe at Equifax, it is apparent that she utterly failed in every meaningful way to plan, implement and audit information security at Equifax. As one analyst noted, "Mauldin failed to ensure that even the most fundamental security principles were in play at Equifax."

28. Operating as a secure storehouse of crucial and highly confidential personal and business financial information is one of Equifax's primary functions and a security breach was a known, obvious and grave risk. Failing to ensure that the Company had proper cybersecurity controls in place to protect the privacy of the consumers whose data it collected and stored; relying on a single individual to take action in response to the warnings, alerts and instructions to install the patch;

failing to monitor whether the patch was installed; and failure to adopt a crisis plan to respond to a major data breach quickly and effectively, were crucial breaches of the Individual Defendants' fiduciary duties – particularly when they were repeatedly warned of the critical vulnerability, the need to take action immediately, and how to do it.

29. In addition, the Individual Defendants further breached their fiduciary duties by causing Equifax to issue false and misleading statements concerning the Company's data security, business practices, operations and internal controls prior to the Data Breach.

30. As a result of the Individual Defendants' wrongful conduct, Equifax has been severely damaged. The Company has been and will continue to be forced to expend large sums of money to provide credit monitoring services for individuals affected by the Breach. It faces enormous liability, damages, penalties and fines in securities, consumer and financial institution class action litigation; numerous other lawsuits and civil enforcement actions by states, cities, and others; investigations by federal and state regulators, congressional committees in both the United States Senate and House of Representatives, 49 state Attorneys General, and British and Canadian governmental authorities; lost business and cancelled contracts; resource constraints; incremental IT and data security costs; legal,

consulting, investigative, and other fees and expenses; severe and lasting damage to the Company's brand and reputation; and the loss of billions of dollars of market capitalization. As Mark W. Begor, the Company's new CEO, stated at a securities analyst conference, a "cloud" sits over Equifax with investors and with our customers.

II. JURISDICTION AND VENUE

31. This Court has original jurisdiction over this action pursuant to 28 U.S.C. § 1331 because Plaintiffs allege claims arising under the laws of the United States. The Court has supplemental jurisdiction over the state law claims asserted herein pursuant to 28 U.S.C. § 1367(a) because they are so related to the claims arising under the laws of the United States that they form part of the same case or controversy. The Court also has diversity jurisdiction over all claims asserted herein pursuant to 28 U.S.C. § 1332 because the plaintiffs and the Individual Defendants are citizens of different states and the amount in controversy exceeds $75,000, exclusive of interest and costs. This action is not a collusive action designed to confer jurisdiction on a court of the United States that it would not otherwise have.

32. This Court has personal jurisdiction over each of the Defendants because each Defendant is either a corporation conducting business and

maintaining operations in this District, or is an individual who is either present in this District for jurisdictional purposes, or has sufficient minimum contacts with this District so as to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

33. Venue is proper in this District pursuant to 28 U.S.C. § 1391. Equifax maintains its principal executive offices in this District. Thus: (i) one or more of the Individual Defendants either resides or maintains executive offices in the District; (ii) a substantial portion of the transactions and wrongs complained of herein occurred in the District; and (iii) the Individual Defendants have received substantial compensation and other transfers of money in the District by doing business and engaging in activities having an effect in the District.

III. PARTIES

A. LEAD PLAINTIFFS

34. Lead Plaintiffs Nancy A.K. and John Weyl are husband and wife and current shareholders of Equifax, were shareholders at the time of the wrongdoing alleged herein, and have been shareholders of Equifax continuously since that time. The Weyls currently own 28,200 shares of Equifax and have continuously held Equifax shares since May of 1994. The Weyls are citizens of New York.

B. DEFENDANTS

1. Nominal Defendant Equifax, Inc.

35. Nominal defendant Equifax is a Georgia corporation with its principal executive offices located at 1550 Peachtree Street N.W., Atlanta, GA. 30309. Equifax common stock trades on the New York Stock Exchange ("NYSE") under the ticker symbol "EFX." Equifax provides information solutions and human resources business process outsourcing services for businesses, governments, and consumers, based on its comprehensive databases of consumer and business information derived from numerous sources. The Company operates through four segments: USIS, International, Workforce Solutions, and Global Consumer Solutions.

36. The USIS segment offers consumer and commercial information services, such as credit information and credit scoring, credit modeling and portfolio analytics, fraud detection and prevention, identity verification, and other consulting, mortgage loan origination information, financial marketing, and identity management services;

37. The International segment provides information service products, which include consumer and commercial services, such as credit and financial information, credit scoring and modeling, and credit and other marketing products

and services, as well as information, technology, and services to support debt collections and recovery management;

38. The Workforce Solutions segment provides employment, income, and social security number verification services; and payroll-based transaction and employment tax management services; and

39. The Global Consumer Solutions segment offers credit information, credit monitoring, and, ironically, identity theft protection products directly to consumers through the Internet and hard-copy formats. Equifax serves customers in financial service, mortgage, human resource, consumer, commercial, telecommunication, retail, automotive, utility, brokerage, healthcare, and insurance industries, as well as state and federal governments.

40. The Company is subject to federal, state, local and foreign laws and regulations concerning, among other things, privacy and data protection. As stated in its Forms 10-K filed with the SEC, "Failure to satisfy those legal and regulatory requirements, or the adoption of new laws or regulations, could have a material adverse effect on our results of operations, financial condition or liquidity."

2. Individual Defendants

41. Defendant Smith was Chairman of the Board and CEO of Equifax from September 2005 until his resignation on September 26, 2017. Smith is a

citizen of Georgia. Smith's total compensation for 2014, 2015, and 2016 was $13,879,675, $12,922,711, and $14,964,563, respectively.

42. Defendant David C. Webb ("Webb") was Chief Information Officer from 2010 until his resignation in September 2017, following the Data Breach. Webb is a citizen of Georgia.

43. Defendant L. Phillip Humann ("Humann") has been a member of the Board since 1992. Humann is a member of the Compensation, Human Resources & Management Succession Committee. Humann's total compensation for 2014, 2015, and 2016 was $226,959, $258,938, and $263,874, respectively. Humann is a citizen of Florida.

44. Defendant Templeton has been a member of the Board since 2008. Templeton is a member of the Audit and Technology Committees. Templeton's total compensation for 2014, 2015, and 2016 was $219,359, $236,308, and $245,050, respectively. Templeton is a citizen of California.

45. Defendant Robert D. Daleo ("Daleo") was a member of the Board from 2006 to May 3, 2018. Daleo was the Chair of the Audit Committee and a member of the Compensation, Human Resources & Management Succession Committee and Executive Committee. Daleo's total compensation for 2014, 2015,

and 2016 was $225,709, $242,688, and $260,996, respectively. Daleo is a citizen of New Jersey.

46. Defendant Siri S. Marshall ("Marshall") has been a member of the Board since 2006. Marshall is the Chair of the Governance Committee and also serves on the Compensation, Human Resources & Management Succession Committee and Executive Committee. Marshall's total compensation for 2014, 2015, and 2016 was $223,279, $242,878, and $252,753, respectively. Marshall is a citizen of California.

47. Defendant Walter W. Driver, Jr. ("Driver") has been a member of the Board since 2007. Driver is a member of the Governance Committee. Driver's total compensation for 2014, 2015, and 2016 was $219,679, $236,628, and $238,867, respectively. Driver is a citizen of Georgia.

48. Defendant McKinley has been a member of the Board since 2008. McKinley is the Chair of the Technology Committee and a member of the Audit and Executive Committees. McKinley's total compensation for 2014, 2015, and 2016 was $225,909, $245,358, and $255,409, respectively. McKinley is a citizen of Virginia.

49. Defendant Feidler has been a member of the Board since 2007. Feidler is the Chair of the Executive Committee and also a member of the

Governance and Technology Committees. Feidler's total compensation for 2014, 2015, and 2016 was $221,959, $239,128, and $255,972, respectively. Feidler is a citizen of Georgia.

50. Defendant Robert D. Marcus ("Marcus") has been a member of the Board since 2013. Marcus is the Chair of the Compensation, Human Resources & Management Succession Committee and a member of the Executive and Governance Committees. Marcus's total compensation for 2014, 2015, and 2016 was $212,159, $229,108, and $241,975, respectively. Marcus is a citizen of New Jersey.

51. Defendant Hough has been a member of the Board since 2016. Hough is on the Audit and Technology Committees. Hough's total compensation for 2016 was $199,474. Hough is a citizen of Georgia.

52. Defendant Stock has been a member of the Board since January 1, 2017. Stock is a member of the Technology Committee. Stock is a citizen of Georgia.

53. Defendant Gamble has been Equifax's Corporate Vice President and CFO since May 2014. On August 1, 2017, Gamble sold 6,500 Equifax shares valued at $946,374, representing about 15% of his Equifax stockholdings. This transaction was not pursuant to a Rule 10b5-1 trading plan. Gamble's total

compensation for 2014, 2015, and 2016 was $7,079,102, $3,053,644, and $3,095,107, respectively. Gamble is a citizen of Georgia.

54. Defendant Loughran is President of Equifax's USIS business. Prior to this role, Loughran was Equifax's Chief Marketing Officer until July 2017. Prior thereto, he was President, Global Consumer Solutions dating back to January 4, 2010. Loughran was also Senior Vice President, Corporate Development from April 2006 to December 2009. On August 1, 2017, Loughran exercised options to sell 7,000 Equifax shares valued at $584,099, representing over 16% of his Equifax stockholdings. This transaction was not pursuant to a Rule 10b5-1 trading plan. Loughran is a citizen of Georgia.

55. Defendant Ploder has been President of Equifax's Workforce Solutions since November 2015. From April 2010 to November 2015, he served as President, USIS. Prior thereto, he served as President, International, from January 2007 to April 2010. From February 2004 to January 2007, he was Group Executive, Latin America. On August 2, 2017, Ploder sold 1,719 Equifax shares valued at $250,458, representing about 4% of his Equifax stockholdings. This transaction was not pursuant to a Rule 10b5-1 trading plan. Ploder's total compensation for 2015 and 2016 was $2,080,109 and $2,760,317, respectively. Ploder is a citizen of Missouri.

56. Defendant Brandberg was the Senior Vice President, Investor Relations of Equifax from February 2017 until February 2018. On August 2, 2017, Brandberg sold Equifax shares valued at more than $250,000. Brandberg is a citizen of Arizona.

57. Defendants Smith, Humann, Templeton, Daleo, Marshall, Driver, McKinley, Feidler, Marcus, Hough, and Stock are referred to herein as the "Director Defendants." Defendants Smith, Gamble, Loughran, Ploder and Brandberg are referred to herein as the "Executive Defendants."

58. The "Director Defendants" and the "Executive Defendants" are collectively referred to herein as the "Individual Defendants."

IV. DUTIES OF THE OFFICERS AND DIRECTORS

59. By reason of their positions as officers, directors, and/or fiduciaries of Equifax and because of their ability to control the business and corporate affairs of the Company, the Individual Defendants owed Equifax and its shareholders fiduciary obligations of trust, loyalty, good faith, candor, due care, and diligence, and were and are required to use their utmost ability to control, manage and oversee Equifax in a fair, just, honest, and equitable manner. The Individual Defendants were and are required to act in furtherance of the best interests of

Equifax and its shareholders so as to benefit all shareholders equally and not in furtherance of their personal interests or benefit.

60. To discharge their duties, the officers and directors of Equifax were required to exercise reasonable and prudent supervision over the management, policies, practices, and controls of the financial and corporate affairs and assets of the Company. By virtue of such duties, the officers and directors of Equifax were required to, among other things:

a. Ensure that the Company complied with its legal obligations and requirements, including complying with regulatory requirements by devising and implementing a system of internal controls sufficient to ensure that consumers' personal and financial information was protected, developing a comprehensive data breach plan, maintaining state of the art technology; timely updating and patching its software and scanning equipment, putting in place adequate encryption and authentication measures, conducting regular cybersecurity audits, and developing a comprehensive crisis management plan;

b. Implement, monitor, maintain and oversee the system of internal controls sufficiently to ensure that consumers' and data providers' personal and financial information was protected;

c. Conduct the affairs of the Company in an efficient, business-like manner so as to make it possible to provide the highest quality performance of its business, to avoid wasting the Company's assets, and to maximize the value of the Company's stock;

d. Remain informed as to how Equifax conducted its operations, and upon receipt of notice or information of imprudent or unsound conditions or practices, make reasonable inquiry in connection therewith, and take steps to correct such conditions or practices as necessary to comply with applicable laws; and

e. Ensure the Company is operated in a diligent, honest, and prudent manner in compliance with all applicable laws, rules, regulations, and industry standards.

61. Board members', as well as officers', duties to implement and maintain effective controls over cyber security were well known to the Individual Defendants. Indeed, Luis A. Aguilar, while an SEC Commissioner, spoke on June 10, 2014, at a "Cyber Risks and the Board" conference as to these very duties, stating:

> Although primary responsibility for risk management has historically belonged to management, the boards are responsible for overseeing that the corporation has established appropriate risk management programs and for overseeing how management oversees those programs. . . . Boards of directors are already responsible for overseeing the management of all types of risk, including credit risk, liquidity risk, and operational risk – and there can be little doubt that cyber-risk also must be considered as part of the board's overall risk oversight.

62. Commissioner Aguilar also noted that "Companies need to be prepared to respond within hours, if not minutes, of a cyber-event to detect the cyber-event, analyze the event, prevent further damage from being done, and prepare a response to the event."

63. Other experts have also emphasized corporate directors' responsibility for ensuring that their company has appropriate and effective risk management programs and the board's responsibility to monitor the implementation of the

programs. For example, Stephen M. Bainbridge, in an article titled *Caremark and Enterprise Risk Management*, 34 Iowa J. Corp. L.967 (2009), wrote: "Although primary responsibility for risk management rests with the corporation's top management team, the board of directors is responsible for ensuring that the corporation has established appropriate risk management programs and for overseeing management's implementation of such programs."

64. Each Individual Defendant, as a director and/or officer, owed to the Company and to its shareholders the fiduciary duties of loyalty, good faith, and candor in the management and administration of the affairs of the Company, as well as in the use and preservation of its property and assets. The conduct of the Individual Defendants complained of herein involves knowing or culpable violations of their obligations as directors and officers of the Company, the absence of good faith on their part, disloyalty to the Company and its shareholders, and a knowing or reckless disregard for their duties to the Company and its shareholders.

V. DUTIES UNDER EQUIFAX'S CHARTER

65. The Board is also required to comply with Corporate Governance Principles detailed on the Company's website. The Corporate Governance Principles describe the Board's mission as:

> [To] serve[] shareholder interests in the management and growth of a successful business, including optimizing long-term financial returns. The Board is responsible for directing the Company in such a way to ensure this result. **This is an active, not a passive, responsibility**. The Board has the responsibility to ensure that in good times, as well as difficult ones, management is capably executing its responsibilities. The Board's responsibility is to regularly monitor the effectiveness of management policies and decisions including the execution of its strategies.

(Emphasis added).

66. As Defendant Smith, the former Chairman and CEO, has admitted, he and his fellow officers and directors "did not live up to that responsibility."

67. Moreover, according to the Company's proxy statement filed with the SEC on March 24, 2017, Equifax's Board "oversees risk management at the Company," and is specifically tasked with "direct oversight of strategic risks to the Company and other risks not delegated to one of its committees."

68. The Board monitors the Company's "tone at the top" and risk culture and oversees emerging strategic risks. "On an annual basis, the Board performs an enterprise risk assessment with management to review the principal risks facing the Company and monitors the steps management is taking to map and mitigate those risks. The Board then sets the general level of risk appropriate for the Company through business strategy reviews. Risks are assessed throughout the business, focusing on (i) financial, operational and strategic risk; and (ii) ethical, legal,

privacy, data security (including cybersecurity), security, regulatory, and other compliance risks."

69. Further, the Board's several standing committees monitor other specific aspects of Equifax's business. Among these committees are the Audit Committee and the Technology Committee. These committees have their own, supplemental charters setting forth duties of their respective members, in addition to their duties as board members generally.

70. In 2017, the Audit Committee was comprised of defendants Daleo, Hough, McKinley, and Templeton.

71. Per the Audit Committee Charter, the Audit Committee's primary function was and is to assist the Board in fulfilling its oversight responsibilities for: (i) the integrity of the Company's financial reporting process and the adequacy and effectiveness of its financial and information technology controls; (ii) the Company's policies related to enterprise risk assessment and risk management; (iii) the Company's systems for complying with legal and regulatory requirements; (iv) the independent auditor's qualifications, independence, and performance; (v) the performance of the Company's internal audit function; and (vi) the integrity of the Company's internal controls regarding finance, accounting, and auditing, and its financial reporting processes.

72. To that end, the Audit Committee has the responsibility to "Review with the Company's principal executive and financial officers, internal auditors and independent auditors the integrity of the Company's financial reporting processes, including . . . any significant deficiencies in the design or operation of internal controls or material weaknesses therein."

73. The Audit Committee also has the responsibility to "Exercise oversight with respect to the structure, operation and efficacy of the Company's regulatory compliance program," including "[a]t least once a year, review and discuss with management the Company's policies with respect to risk assessment and risk management, including, without limitation, material regulatory, compliance and litigation risks facing the Company" and to direct management to take appropriate steps to monitor and mitigate such exposures and policy concerns."

74. The responsibilities of the Audit Committee also include:

* Regular review of compliance with applicable laws and regulations;

* Approval of the annual compliance audit plan and review of such audits to be performed by the Internal Audit department of the Company; and

* Review of significant inquiries received from regulators or government agencies, including, without limitation, issues pertaining to federal or state securities or consumer financial protection laws or

> regulations or enforcement or other actions brought or threatened to be brought against the Company by, regulators or government agencies.

75. The Technology Committee is comprised of defendants McKinley, Feidler, Hough, Stock, and Templeton.

76. Per the Technology Committee Charter, the Technology Committee's responsibilities include "provid[ing] guidance on technology as it may pertain to, among other things . . . security concerns." The Technology Committee was required to:

> [R]eview and monitor the Company's technology strategy and significant technology investments in support of its evolving global business needs. Areas of review include: information technology strategy; significant new product lines or technology investments; and the Company's response to external technology-based threats and opportunities. In addition, the Committee will oversee the Company's mitigation of any identified enterprise-wide risks in the above areas.

77. As stated in the Company's Proxy Statement filed with the SEC on March 24, 2017, the Technology Committee "Focuses on technology related risks and opportunities, including data security."

78. Moreover, the Technology Committee is and was charged with monitoring the Company's long-term strategy and significant investments in the following areas:

> 1. Information technology long-term strategy in support of the Company's evolving global business needs.

2. Review and present observations to the Board with respect to the annual technology budget.

3. Significant new product development programs (including software initiatives) and new technology investments, including technical and market risks associated with product development and investment.

4. Future trends in technology that may affect the Company's strategic plans, including overall industry trends and new opportunities and threats occasioned by new technologies, especially disruptive technologies.

5. Review the Company's technology investments and infrastructure associated with risk management, including policies relating to information security, disaster recovery and business continuity.

6. Assess the scope and quality of the Company's intellectual property.

7. Undertake from time to time such additional activities within the scope of the Committee's primary purposes as it may deem appropriate and/or as assigned by the Board of Directors, the Chairman of the Board and Chief Executive Officer.

VI. DUTIES UNDER EQUIFAX'S CODE OF ETHICS AND BUSINESS CONDUCT

79. Equifax's Code of Ethics and Business Conduct, which applies to all of the Individual Defendants, provides, in pertinent part:

> Violating relevant laws, regulations or the Code, or encouraging others to do so, exposes the Company to liability and puts our reputation at risk. If an ethics or compliance problem does occur, you are required to report it so that an effective solution can be developed.

* * *

One of our most valuable assets is information. Each of us must be vigilant and protect confidential information. This means keeping it secure, limiting access to those who have a need to know in order to do their job, and avoiding discussion of confidential information in public areas. . . . Confidential information includes all non-public information that might be of use to competitors, or harmful to the Company or its customers, if disclosed.

* * *

Our customers and our business partners place their trust in us. We must protect their confidential information. MAKE SURE YOU: Learn about the types of information which are given heightened protection by the law and Company policy (such as personally identifiable information, like social security numbers and bank account numbers) and protect them through appropriate means (such as encryption or other types of limited access). Never share confidential information inside or outside the Company except as authorized. Immediately report any loss or theft of confidential information.

* * *

Business partners, government officials and the public need to be able to rely on the accuracy and completeness of our disclosures and business records. Accurate information is also essential within the Company so that we can make good decisions. Our books and records must be clear, complete and in compliance with accepted accounting rules and controls. Employees with a role in financial or operational recording or reporting have a special responsibility in this area, but all of us contribute to the process of recording business results and maintaining records. Each of us is responsible for helping to ensure the information we record is accurate and complete and maintained in a manner that is consistent with our system of internal controls. If you suspect any irregularity relating to the integrity of our

> records, you need to report it immediately to your supervisor, the Legal Department or the Corporate Ethics Officer.
>
> * * *
>
> Insider Trading
>
> No Equifax employee, officer, director or other "insider" may purchase or sell Equifax securities while in possession of material, nonpublic information relating to Equifax ("insider trading").

80. Finally, Equifax touted its privacy protocols in its "Privacy Policy" posted on its website. The Privacy Policy states that Equifax has:

> [B]uilt our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax.

(Emphasis added).

VII. DUTIES UNDER GEORGIA LAW

81. As officers and directors of a Georgia corporation, the Individual Defendants were required to discharge their duties in good faith and "with the care an ordinarily prudent person in a like position would exercise under similar circumstances." O.C.G.A. § 14-2-830(a)(1), (2) (directors) and § 14-2-842(a)(1), (2) (officers).

82. Equifax's officers and directors were also required, pursuant to the Georgia Security Breach Notification Act, O.C.G.A. §§ 10-1-912, *et seq.*, to notify affected person's "in the most expedient time possible and without unreasonable delay."

83. Finally, O.C.G.A. § 51-1-6 provides: "When the law requires a person to perform an act for the benefit of another or to refrain from doing an act which may injure another, although no cause of action is given in express terms, the injured party may recover for the breach of such legal duty if he suffers damage thereby."

VIII. DUTIES UNDER FEDERAL LAWS

84. The Financial Services Modernization Act of 1999, commonly known as the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. §§ 6801, *et seq.*, mandates that Equifax, like other financial institutions and credit bureaus, "protect the security and confidentiality" of the non-public personal information it collects. Equifax is required to "develop, implement, and maintain a comprehensive security program" that "contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue."

85. The FTC, pursuant to the Standards for Safeguarding Customer Information Rule (the "Safeguards Rule"), 16 C.F.R. Part 314, implementing Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), is responsible for enforcing compliance with the GLBA and regularly publishes security guidance and enforcement decisions. Breach of the GLBA can result in civil and/or criminal liability and sanctions by regulatory authorities, including fines of up to $100,000 per violation.

86. The Safeguards Rule requires Equifax to develop a comprehensive written information security program that contains reasonable safeguards, including identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; to assess the sufficiency of any security program safeguards in place to control those risks and regularly monitor the effectiveness of the safeguards; and to make changes and adjustments to the safeguards based upon the testing, monitoring, and other relevant circumstances.

87. Equifax is also subject to the Fair Credit Reporting Act ("FCRA"), 18 U.S.C. §§ 1681, *et seq*., which, among other things, governs the privacy of information in the files of consumer reporting agencies ("CRA"). The FCRA requires:

> [T]hat consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information.

88. Reasonable data security measures are also mandated by state security breach statutes in states where Equifax does business.

89. Equifax's independent registered public accounting firm, Ernst & Young, in its publication titled "2016 SEC annual reports – Form 10-K," advised Equifax that SEC disclosure rules apply to "cybersecurity risks and incidents that could have a material effect on a registrant's financial statements."

IX. SUBSTANTIVE ALLEGATIONS

A. EQUIFAX'S BUSINESS

90. Equifax is one of three CRAs in the United States that compile and maintain data concerning consumers and businesses on a nationwide basis. As such, Equifax collects, maintains, and sells comprehensive and highly sensitive personal data of consumers and businesses, including, in addition to their PII, account numbers, social security numbers, loan information (including original loan amounts and dates, balances, past due amounts, current status and payment history), credit card accounts (including credit limit, balances, past due amounts, current status and payment history), as well as information on everything from

child support payments, missed or past due rent and utilities payments, bankruptcy history, liens, addresses, telephone numbers, and employment history. All of this information, and more, factors into credit scores and can and does affect the availability of credit, the terms upon which credit is offered, insurance underwriting, and employment, and other financial decisions.

B. THE INDIVIDUAL DEFENDANTS HAVE LONG RECOGNIZED THE IMPORTANCE OF CYBERSECURITY TO EQUIFAX AND ITS CUSTOMERS

91. Equifax has long acknowledged the importance of protecting consumer privacy. In its Form 10-K filed with the SEC on March 12, 2002, Equifax stated:

> Because our business involves the collection of consumer and business data and distribution of such information to businesses making credit and marketing decisions, certain of our activities and services are subject to regulation under various U.S. federal laws including the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, as well as similar state laws. We are also subject to privacy and consumer credit laws and regulations in foreign countries where we do business. It is the Company's policy to treat all information with a high degree of security reflecting our recognition of individuals' privacy concerns.

92. Equifax further identified the potential repercussions of a data security breach as a substantial "Risk Factor" for its business in its Forms 10-K filed with the SEC on March 28, 2003 and March 11, 2004, stating: "Security is important to

our business, and breaches of security, or the perception that e-commerce is not secure, could harm our business."

93. As the world became more technologically advanced, so too did Equifax's recognition of the importance of securing individuals' personal information. As noted in its Form 10-K filed with the SEC on February 26, 2009 and in its Forms 10-K for subsequent years:

> INFORMATION SECURITY AND GOVERNMENT REGULATION
>
> Safeguarding the privacy and security of consumer credit information, whether delivered online or in an offline format, is a top priority. We recognize the importance of secure online transactions and we maintain physical, administrative, and technical safeguards to protect personal and business identifiable information. We have security protocols and measures in place to protect information from unauthorized access or alteration. These measures include internal and external firewalls, physical security and technological security measures, and encryption of certain data.
>
> Our databases are regularly updated by information provided by financial institutions, telecommunications companies, other trade credit providers, public records vendors and governments. Various laws and regulations govern the collection and use of this information. These laws and regulations impact how we are able to provide information to our customers and have significantly increased our compliance costs. We are subject to differing laws and regulations depending on where we operate.

C. THE INDIVIDUAL DEFENDANTS HAVE LONG KNOWN THAT EQUIFAX IS "REGULARLY THE TARGET OF ATTEMPTED CYBER AND OTHER SECURITY THREATS" AND THE REPERCUSSIONS

94. In its Forms 10-K filed with the SEC for the years 2013, 2014, 2015 and on February 22, 2017 (the "2016 10-K"), Equifax acknowledged the known risk of a security breach and how any potential breach could have serious repercussions for the Company:

> ***Security breaches and other disruptions to our information technology infrastructure could interfere with our operations, and could compromise Company, customer and consumer information, exposing us to liability which could cause our business and reputation to suffer.***
>
> * * *
>
> **Serve as a trusted steward and advocate for our customers and consumers.** This includes continuously improving the customer and consumer experience in our consumer and commercial offerings, anticipating and executing on regulatory initiatives, while simultaneously delivering security for our services.

(Emphasis in original).

95. The Individual Defendants also acknowledged in the Company's SEC filings that:

> **We are regularly the target of attempted cyber and other security threats and must continuously monitor and develop our information technology networks and infrastructure** to prevent, detect, address and mitigate the risk of unauthorized access, misuse, computer viruses and other events that could have a security impact. . . . Any such access, disclosure or other loss of information

> could subject us to litigation, regulatory fines, penalties or reputational damage, any of which could have a material effect on our cash flows, competitive position, financial condition or results of operations.

(Emphasis added).

96. Indeed, as reported by *Bloomberg* in a September 2017 article: "In the corridors and break rooms of Equifax's giant Atlanta headquarters, employees used to joke that their enormously successful credit company was just one hack away from bankruptcy."

97. In keeping with the importance that the Individual Defendants acknowledged in the Forms 10-K must be placed on the protection of customer personal information, during a speech given by defendant Smith at the University of Georgia on August 17, 2017, three months after the Data Breach occurred, but before it was disclosed to the public, Smith, who was "in charge of overseeing" the Company's consumer databases and the cyber threats to its information systems, stated: "When you have the size database we have, it's very attractive for others to try to get into our database," and thus "it is a **huge priority** for us." (Emphasis added).

98. In its 2017 Proxy Statement, Equifax represented: "We have a **rigorous enterprise-wide risk management program** ('ERM') targeting controls over operational, financial, legal/regulatory compliance, reputational, technology,

privacy, **data security**, strategic and other risks that could adversely affect our business. The program also includes **crisis management** and business continuity planning." The Company added that: "Our CEO and senior leadership team receive comprehensive periodic reports on the most significant risks from the director of our internal audit department." (Emphasis added). The 2015 and 2016 Proxy Statements contained the same or similar representations.

99. In truth, however, as subsequent events demonstrated, data security was not a "huge priority" for Equifax, the Individual Defendants did not establish a "rigorous" enterprise risk or crisis management program," and, as such, caused Equifax to breach its obligations as a "trusted steward" for consumers and businesses.

D. CYBERATTACKS ON THE RISE

100. PII is a very valuable commodity to identity thieves. As the FTC has recognized, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[1]

[1] *See* FTC, Warning Signs of Identity Theft, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited July 9, 2018).

101. Legitimate businesses and the criminal underground alike recognize the value in PII contained in a merchant's data systems, and both have aggressively sought out the information since the advent of the internet. *The New York Times*, in a May 21, 2018 article titled "War Rooms Help Banks on Cybercrime," noted:

> Cybercrime is one of the world's fastest-growing and most lucrative industries. At least $445 billion was lost last year, up around 30 percent from just three years earlier, a global economic study found, and the Treasury Department recently designated cyberattacks as one of the greatest risks to the American financial sector. For banks and payment companies, the fight feels like a war – and they're responding with an increasingly militarized approach.

102. Brian Vecci, a cybersecurity expert, stated to *The Wall Street Journal* in September 2017, that names, addresses, social security numbers and the other information maintained by Equifax and other credit bureaus are "the keys to the digital kingdom. If I have all that, I can probably walk to the bank and get a mortgage with it."

E. EQUIFAX EXPERIENCED PREVIOUS SECURITY BREACHES AND CYBERATTACKS

103. Although protecting consumer data is essential to Equifax's primary corporate purpose and the Company has repeatedly emphasized the importance of data security, the Company's Officers and Directors knew or turned a blind eye to the fact that Equifax's cyber security was lagging. The Company has systematically experienced problems protecting consumers' information dating

back years. Collectively, these security breaches – and specific warnings from consultants and third parties – put the Board on notice that they had failed to implement effective security systems, practices, defenses, and monitoring and that Equifax was highly susceptible to a data breach.

104. Despite the Company's repeated representations regarding the importance of protecting its consumers' information, the Individual Defendants have for years ignored Equifax's lax and ineffective internal controls and systemic data protection deficiencies. In early 2010, tax forms mailed by Equifax's payroll vendor through the United States Postal Service had each employee's Social Security number in a control number field, which was partially to fully viewable through the return address window. This allowed anyone in possession of the envelope to view the Social Security number without opening it. Coretha Rushing, the Chief Human Resource Officer at Equifax, described the breach in a letter, stating: "Control Numbers were intended to be a unique number, not a SSN. . . . We apologize for the incident and we are exploring various avenues so this does not happen again."

105. An Equifax employee whose Social Security number was exposed in the incident called Equifax negligent and expressed concern that it reflected poorly on Equifax's reputation as a company engaged in the business of helping

consumers to protect themselves from identity fraud. The employee said, "If they can't do this internally how are they going to be able to go to American Express and other companies and say we can mitigate your liability? . . . They are first-hand delivering information for the fraudsters out there. . . . It's so terribly sad. It's just unacceptable, especially from a credit bureau."

106. In March 2013, Equifax confirmed "fraudulent and unauthorized access" to the financial files of four high-profile people, but declined to identify the individuals. Tim Klein, an Equifax spokesman, stated, "We are aware of recent media reports pertaining to unauthorized access to files belonging to high-profile individuals. Equifax can confirm that fraudulent and unauthorized access to four consumer credit reports has occurred." Around the same time, the U.S. Secret Service announced an investigation into the potential hacking of then First Lady Michelle Obama, then Vice President Joe Biden, former Secretary of State Hillary Clinton, then FBI Director Robert Mueller, then U.S. Attorney General Eric Holder, and former Alaska Governor Sarah Palin. The hack appears to have originated in Russia by the use of publicly available information to answer security questions and bypass authentication measures.

107. In 2014, Equifax retained KPMG, a professional accounting firm, to conduct a security audit. KPMG alerted Equifax and the Individual Defendants

that the Company's encryption protocols were grossly inadequate to protect PII. It noted that the Company stored encryption keys on the same public network servers on which it maintained the encrypted data.

108. Notwithstanding KPMG's admonition that the encryption keys and the data must be separated, Equifax and the Individual Defendants failed to take this critical cybersecurity measure.

109. In March 2014, Equifax admitted to the Attorney General of New Hampshire that its security team had discovered a suspicious pattern of inquiries originating from a single IP address from April 2013 to January 31, 2014. The Company stated that someone at the IP address may have made unauthorized inquiries to Equifax for credit reports and that credit reports may have been fraudulently ordered by the IP address operator. The IP address operator was able to obtain the credit reports because it had obtained sufficient PII to meet Equifax's identity verification process. This was the result of the Individual Defendants' failure to implement adequate and necessary monitoring and security safeguards.

110. In early 2015, hackers penetrated Equifax's W-2 Express website. Equifax's "monitoring" failed to detect the breach for approximately one year, resulting in the leak of 430,000 names, addresses, Social Security numbers, and other personal information from Kroger supermarket employees. In class action

litigation which ensued, the plaintiffs argued that Equifax had "willfully ignored known weaknesses in its data security, including prior hacks into its information systems." The case was subsequently settled, with Equifax agreeing to fix a glaring security issue, which arose from Equifax's decision to have Kroger supermarket employees and employees of other companies access their data with the use of default PIN numbers. The PINs, according to the plaintiff's complaint, consisted of the last four digits of an individual's social security number and their four-digit year of birth to provide authentication. A determined hacker could gather such information by scouring the web, or duping a target into disclosing the information. In the settlement, Equifax agreed to stop using the default PINs. Despite that agreement, it failed to employ this critical security measure. Equifax continued to use simple PINs after that settlement in September 2016 and failed to use adequate and necessary authentication protocols.

111. In early 2017, Equifax disclosed that its subsidiary, Equifax Workforce Solutions, also known as TALX Corporation ("TALX"), which provides online payroll, HR, and tax services, had its W-2 Express website breached. Because of Equifax's almost non-existent monitoring, this breach also continued for a year, from April 2016 through March 2017, before it was detected.

The primary purpose of a service like TALX is to securely manage employee data; Equifax failed on that front.

112. In May 2017, independent cybersecurity reporter Brian Krebs explained that hackers were able to file fraudulent tax returns and steal tax refunds from employees of companies that used TALX for HR and tax services. The hackers were able to reset individuals' 4-digit PIN numbers by using personal information to correctly answer the required personal questions.

113. In a May 15, 2017 letter to the New Hampshire Attorney General, Equifax stated that it was unable to determine how many tax records were hacked. It assured the Attorney General that "to help prevent recurrence of this type of incident, TALX has implemented additional security measures, including **enhanced fraud monitoring** and removal of personal questions as an option to reset PINs from the online portal." (Emphasis added). It provided this assurance notwithstanding its agreement a year earlier to refrain from using personal identifiers as part of its authentication process. It further assured the Attorney General that it would implement two-factor authentication, which cybersecurity experts had long advised Equifax was essential to establishing adequate cybersecurity of PII.

114. Notwithstanding its assurances to the New Hampshire Attorney General and its settlement agreement in the W2Express litigation, Equifax continued to use personal identifiers in its security protocols for TALX data. Equifax continued to employ Social Security numbers as user names and birth dates served as passwords.

115. On May 18, 2016, at a Barclays analyst conference, Smith was asked "How do you guys make sure the data doesn't bleed?" He responded: "We have a world-class team; we never take for granted our need to continue to innovate around data security. I think we are in a very good position now, but you can never become complacent about security, because a lot of people with a lot of time on their hands are trying to crack that database."

116. In 2016, a security researcher found a common vulnerability known as cross-site scripting ("XSS") on the main Equifax website. Such XSS bugs allow attackers to send specially-crafted links to Equifax customers and, if the target clicks through and is logged into the site, their username and password can be revealed to the hacker.

117. The gross inadequacy of Equifax's data security protection was again confirmed by its own expert, Mandiant Corporation ("Mandiant"), the computer forensics division of cybersecurity firm FireEye. As reported by *Bloomberg* on

September 29, 2017, "Mandiant warned Equifax that its unpatched systems and misconfigured security policies could indicate major problems, a person familiar with the perspectives of both sides said."

118. Mandiant's warning and advice were rejected by Equifax and the Individual Defendants. As *Bloomberg* reported, they "squelched a broader review of [Equifax's] security posture," which "looks to have given the intruders room to operate freely within the company's network for months."

119. Similarly, Equifax and the Individual Defendants rejected the warning and advice of Deloitte, the accounting and consulting firm hired by Equifax to perform a security audit in 2016. *Motherboard* reported in an October 26, 2017 article titled "Equifax Was Warned," that: "The audit found several problems, including a careless approach to patching systems," according to a former Equifax cybersecurity employee. "Nobody took that security audit seriously," the former employee said.

120. The *Motherboard* article also reported that a security researcher warned Equifax in December 2016 that one of its public-facing websites "displayed several search fields, and anyone – with no authentication whatsoever – could force the site to display [consumers'] personal data," including Social Security numbers, full names, birthdates, and city and state of residence. The

researcher explained that the "site looked like a portal made only for employees, but was completely exposed to anyone on the internet. . . . All you had to do was put in a search term and get millions of results, just instantly – in cleartext [*i.e.*, unencrypted], through a web app." He further informed Equifax that "the data of hundreds of thousands of Americans" was downloaded "in order to show Equifax the vulnerabilities within its systems." The researcher told *Motherboard*, "I've seen a lot of bad things, but not this bad."

121. According to an October 6, 2017 *Wall Street Journal* article titled, "A Warning Shot on Equifax: Index Provider Flagged Security Issues Last Year," MSCI, Inc. ("MSCI"), an investment research firm, warned in August of 2016, more than six months prior to the Data Breach, that Equifax was not equipped for the "increasing frequency and sophistication of data breaches." After poring over Equifax's records, MSCI said it found zero evidence that the Company conducted regular cybersecurity audits or provided training to employees on identifying risks, nor did it have any emergency plans to handle a data breach or leak. Due to these cybersecurity concerns, MSCI removed Equifax from its stock indices, which evaluate companies based on environmental, social, and governance criteria. "If you're an investor or asset manager and you see these rock-bottom evaluations of Equifax, it had to have given you pause," Jon Hale, head of sustainability research

at Morningstar Inc., an investment research and investment management firm, told *The Wall Street Journal*.

122. In December 2016, MSCI issued a follow-up research report which stated: "Equifax is vulnerable to data theft and security breaches, as is evident from the 2016 breach of 431,000 employees' salary and tax data of one of its largest customers, Kroger grocery chain. The company's data and privacy policies are limited in scope and Equifax shows no evidence of data breach plans or regular audits of its information security policies and systems."

123. That same month, Equifax was warned by a security researcher that one of its public-facing websites "displayed several search fields, and anyone – with no authentication whatsoever – could force the site to display the personal data of Equifax's customers." Indeed, the researcher promptly reported to Equifax that its servers were running outdated technologies and software vulnerable to breaches and that he was able to access in cleartext, *i.e.*, unencrypted, the names, Social Security numbers, birth dates, and city and addresses for "every American" through Equifax's unsecured website. "It should've been fixed the moment it was found," the researcher said. "It would have taken them five minutes." Nevertheless, the researcher's findings were ignored and the security vulnerability was left unchecked.

124. In January 2017, Equifax revealed a data leak in which credit information of a "small number" of customers at partner LifeLock, an identity-protection company, had been exposed to other users of its online portal.

125. In April 2017 – the month before the Data Breach – Cyence, a cyber-risk analysis firm, rated the possibility of a data breach at Equifax during the next 12 months at 50%. It also found that the Company performed poorly when compared with other financial-services companies.

126. Given the critical importance to Equifax's business of vigilantly protecting consumer information, as repeatedly recognized in public representations, the Individual Defendants had a duty to investigate and take action when put on notice of misconduct that jeopardized the Company's ability to fulfill that mission. Equifax's history of numerous data breaches, lax and ineffective safeguards and controls, inadequate monitoring, and outdated software, well demonstrate that the Individual Defendants failed to investigate and take action. The Individual Defendants had a fiduciary duty – indeed, a heightened fiduciary duty – to be hyper-vigilant, to put in place effective safeguards and monitoring, to heed specific warnings and alerts, to regularly patch and update its software, and to prevent future breaches and protect sensitive customer and consumer data.

Unfortunately, rather than being red flags that spurred the Individual Defendants to action, the earlier breaches were a prelude to the Data Breach.

F. THE BREACH AND EQUIFAX'S RESPONSE

127. Equifax used "Apache Struts" open-sourced web application software. Accordingly, the responsibility to download and load patches rested with Equifax. On March 7, 2017, the Apache Software Foundation issued two security bulletins advising of critical security vulnerabilities in the Apache Struts software, identified as CVE-2017-5638. The Apache Software Foundation's March 7, 2017 security bulletins S2-045 and S2-046 ranked the vulnerability as "***critical***," the "maximum security rating." It released new versions of its software the following day, and advised all "Struts 2 developers and users" to upgrade to the new versions, which contained a security patch.

128. On March 8, 2017, the Department of Homeland Security and Cisco Systems, Inc., each also warned of the specific vulnerability. Cisco reported that it found "a high number" of examples where the vulnerability had already been exploited. Indeed, the information concerning the Apache Struts vulnerability was posted to FreeBuf.com, a Chinese security website, and to Metasploit, a hacking tool.

129. That same day, March 8, 2017, a financial firm concerned about the vulnerability of Apache Struts expressly asked Equifax whether it installed the new security patch. As reported by *The Wall Street Journal* on September 18, 2017, Equifax responded that "it didn't have an issue."

130. The following day, March 9, 2017, the Department of Homeland Security Computer Emergency Readiness Team ("CERT") emailed Equifax directly with a warning that the vulnerability in Apache Struts was of "high" severity and specifically instructing Equifax to install the patch. Although Equifax's policies mandated that it install any security patch within two days of notification of the risk, Equifax did not install the Apache Struts patch. Defendant Smith testified to the United States Senate that Equifax disseminated the CERT warning the next day and ran a scan of its computer network on March 15, 2018, and another scan thereafter. However, Equifax's scans were performed with old and outdated technology and did not test Equifax's full system. Therefore, they did not reveal any problems.

131. That same day, March 9, 2017, numerous widely-read publications also warned of the dangerous vulnerability and the urgent need for companies using Apache Struts to download and install the patch. Professor Jamie Winterton, Director of Strategy at Arizona State University's Global Security Initiative, later

told the Senate that patching is "possibly the most important piece of a company's security posture." He noted:

> Some organizations have implemented **weekly or daily patching** procedures for critical vulnerabilities in exposed systems. The organization's systems should be subject to **regular, consistent monitoring and review** – if a patch is available but not installed, that problem should be discovered promptly, elevated, and the risks assessed accordingly. Patching isn't just an IT problem; it has organizational-level impacts on compliance as well as operational efficiency – so the patch strategy, with its benefits and risks, should be well understood at the C-suite level.

(Emphasis added).

132. Also on March 9, 2017, *Ars Technica*, under the headline "Critical vulnerability under 'massive' attack imperils high-impact sites," warned of a "string of attacks that have escalated over the past 48 hours [where] hackers are actively exploiting a critical vulnerability that allows them to take almost complete control of Web servers used by banks, government agencies, and large Internet companies." *The Register* reported "Apache Struts 2 Needs Patching Now, Without Delay. It's Under Attack Now." *PC World* headlined "Hackers Exploit Apache Struts Vulnerability to Compromise Corporate Web Servers."

133. Yet another warning came the following day, March 10, 2017, when the National Institute of Standards and Technology ("NIST") of the United States Department of Commerce warned of the vulnerability on its National Vulnerability

Database, listing its severity as 10, the highest severity level. NIST's warning directed Apache Struts users to certain identified web sites for solutions and tools to fix the vulnerability.

134. Notwithstanding all of these urgent warnings and alerts of the severity of the vulnerability and the high risk that the extremely sensitive and valuable data maintained by Equifax would be stolen, and notwithstanding the ease with which the vulnerability could be eliminated, Equifax failed to install the patch or take other necessary measures to protect against the flaw.

135. On May 13, 2017, hackers began actively exploiting the known and unpatched vulnerability. They continued to do so at their leisure, having unfettered access to Equifax's computer systems for another 77 days until the Data Breach was finally detected by the Company on July 29, 2017. During that period, hackers had unlimited access to Equifax's systems and were able to steal the PII of half of all Americans and of numerous consumers around the world.

136. *Bloomberg* reported in a September 29, 2017 article that:

> According to an internal analysis of the attack, the hackers had time to customize their tools to more efficiently exploit Equifax's software, and to query and analyze dozens of databases to decide which held the most valuable data. The trove they collected was so large it had to be broken up into smaller pieces to try to avoid tripping alarms as data slipped from the company's grasp through the summer.

137. Equifax has released a chart which approximates by category the number of United States consumers whose personal information was stolen, as follows:

Name	146.6 million
Date of Birth	146.6 million
Social Security Number	145.5 million
Address Information	99 million
Gender	27.3 million
Phone Number	20.3 million
Driver's License Number	17.6 million
Email address	1.8 million
Credit Card Number	209,000
Tax ID	97,500

138. On July 30, 2017, almost four months after being repeatedly warned to do so, Equifax finally patched the vulnerability and ended the Data Breach.

139. Smith testified that he learned of the Data Breach on July 31, 2017. Just 48 hours later, Equifax enlisted the help of King & Spalding and the law firm's data security team. Nevertheless, Smith waited over two weeks, until August 15, 2017, to request a briefing from Equifax's forensic investigators.

140. On August 17, 2017, after being briefed regarding the Data Breach, Smith gave a breakfast speech at the Terry College of Business at the University of Georgia. On that day, Smith had been informed that a "forensic investigation had determined that there were large volumes of consumer data that had been compromised," exposing personal information belonging to almost 150 million people. But, in his speech at Terry College, Smith failed to mention the Data Breach.

141. Channel 2 News of Atlanta reported that during his August 17, 2017 speech, Smith boasted of Equifax's financial and data management achievements. He capped off his statements by saying, "I'm convinced if this team continues to stay focused, the days are bright for Equifax." When specifically asked about data fraud and security, Smith, who two days earlier had requested a "detailed briefing" of the intrusion, stated, "Fraud is a huge opportunity for us. It is a massive, growing business for us." Smith also spoke about how attractive Equifax's database was to hackers, stating, "The flip side is, when you have the size database we have, it's very attractive for others to try to get into our database, so it's a huge priority for us, as you might guess."[2]

[2] Smith's speech is available at https://youtu.be/lZzqUnQg-Us (last visited July 9, 2018) and incorporated herein.

142. Anyone who guessed that database security was a "huge priority" for Equifax, guessed wrong.

143. One observer, Edward Queen of Emory University's Center for Ethics, observed that Smith's answer suggested a level of arrogance and disregard. Mr. Queen went on to say, "The disturbing thing was that he responded the way he did to the question of security breaches, about data breaches, when he knew that the company had already suffered a massive one."

144. The Equifax Board of Directors was not notified of the Data Breach until August 24, 2017, three and a half weeks after Smith learned of it. The Board met for the first time to discuss the matter a week later, on September 1, 2017.

145. On August 1-2, 2017, shortly after the Company learned of the Data Breach, defendants Gamble, Loughran, Ploder and Brandberg, after learning about the size and scope of the Data Breach, unloaded large quantities of Equifax securities. The Individual Defendants did not inform consumers whose confidential personally identifiable information was stolen of the Data Breach until September 7, 2017, forty days after Equifax discovered the breach.

146. Equifax told the public about the Breach in a September 7, 2017 press release. The press release read as follows:

> Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.
>
> The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents. Equifax will work with UK and Canadian regulators to determine appropriate next steps. The company has found no evidence that personal information of consumers in any other country has been impacted.
>
> Equifax discovered the unauthorized access on July 29 of this year and acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.

147. In total, although Equifax's policy required that the patch be installed within 48 hours after receiving the warning and instruction to do so, Equifax took 144 days from March 7, 2017, when the critical vulnerability was first discovered, to patch it; 77 days from when hackers began exploiting the vulnerability on May

13, 2017 to notice that its data had been compromised; and 117 days from when the Breach began and 40 days from when it was discovered to inform consumers and the public.

148. The public outrage was a firestorm. While there have been recent cyberattacks at other companies, the scope of the Breach at Equifax eclipsed all other attacks because of its severity. In the Breach, thieves were able to steal far more PII than in previous hacks, though it is hard not to see that the recurring cyberattacks were building towards such a compromise. The Breach essentially included the keys that unlock consumers' financial and medical histories, bank accounts, employee accounts, and tax information. Using the data stolen from Equifax, identity thieves can impersonate people with lenders, creditors, and service providers who rely on PII from Equifax to make financial decisions regarding potential customers.

149. Analysts agreed that the cyberattack on Equifax was of a magnitude unlike any other, and they laid the blame squarely at the feet of the Individual Defendants. "On a scale of 1 to 10 in terms of risk to consumers, this is a 10," said Avivah Litan, a cybersecurity and fraud analyst at Gartner Inc. Ms. Litan and other cybersecurity professionals criticized Equifax for not improving its security practices after the previous breaches at the Company, and they noted that thieves

were able to get the Company's crown jewels through a simple website vulnerability. Ms. Litan also pointed out that Equifax should have had multiple layers of controls, so even if hackers managed to break in, they could be stopped before doing too much damage.

150. The Company also received harsh criticism and ridicule for its delayed disclosure of the cyberattack. The fact that Equifax discovered the Breach on July 29, 2017, but did not disclose the theft of personal data until September 7, 2017, runs counter to the requirement that public companies are to report promptly any new information that could materially affect their financial outlook.

151. "It's pretty remarkable how long Equifax has been aware of the problem and did not disclose it," said Eric Chaffee, a law professor at the University of Toledo and editor of the Securities Law Blog. "The main problem here is the failure to disclose a catastrophic cyberattack that compromised the information that is at the heart of Equifax's business model. This created a duty to disclose this attack in a timely fashion to investors, potential investors, and those whose data was compromised."

152. Incredibly, Equifax's 2018 Proxy Statement and its Form 10-K and Annual Report for the year ended December 31, 2017, filed with the SEC and disseminated to shareholders, falsely stated: "The Company acted promptly to

notify the approximately 145.5 million U.S. consumers whose personally identifiable information the Company had identified in 2017 as potentially accessed."

153. Clearly, Equifax's much vaunted security safeguards and protections, its monitoring and internal controls, its computer software, its data risk skills, expertise and management, and commitment to security, were profoundly and fundamentally flawed, outdated and not in compliance with industry standards or the Company's representations to its customers and the public.

154. Equally clear, the Individual Defendants breached their fiduciary duties to Equifax to take action when presented with circumstances that posed a threat to the Company's financial condition and business prospects. The Individual Defendants were required to ensure that the Company properly secured consumer data; that it maintained state of the art technology and updated software, scanning equipment, and systems patching; that it tested security systems and processes on a daily basis; that it timely responded to software and system weakness and vulnerability and to patching warnings and alerts; that it monitored and confirmed compliance with instructions and warnings to protect against vulnerabilities and threats; that it encrypted data; that it implemented network segmentation between internet facing systems and backend databases and data

stores; that it had in place firewalls and redundancies to protect data; that it had strong authentication, detection, prevention, and recovery controls; that it regularly tested and monitored the network for unusual and unauthorized activity; that it had endpoint detection software to prevent exfiltration of data; that it had an effective crisis management plan; and that it promptly notified consumers in the event of a breach.

155. On September 15, 2017, Equifax announced that Chief Information Security Officer Susan Mauldin and Chief Information Officer David C. Webb would "retire."

156. On September 26, 2017, the Board announced that defendant Smith would "retire" as Equifax's Chairman and CEO, effective immediately. Notably, according to *Fortune*, Smith retired from Equifax with a payday worth as much as $90 million. Specifically, Smith has already received approximately $72 million (including nine months of his $1,450,000 salary), and he will receive another $17.9 million over the next few years as his stock compensation vests (collectively, these awards are referred to herein as the "Retirement Agreement").

157. Despite his prominent role in allowing the Breach to occur, and then concealing it, Smith was allowed to retire from Equifax, as opposed to being terminated for cause, so that he would earn his unvested stock compensation,

including options and performance-based awards, as though he were still working at the Company.

158. Smith's Retirement Agreement is excessive, unwarranted, and serves no legitimate business purpose, particularly in light of Smith's breaches of fiduciary duty in connection with the Breach, knowingly failing to heed the numerous warnings, alerts and instructions, knowingly failing to monitor whether the instructions had been implemented, and knowingly failing to timely inform the Board, regulators and the public. Essentially, Smith is being rewarded with a $90 million payday despite the Company incurring significant damage from the Breach, which occurred on his watch and as a result of his breaches of fiduciary duty as CEO and Chairman.

159. On September 27, 2017, Paulino do Rego Barros, Jr. ("Barros"), the newly appointed interim CEO, published an op-ed article in *The Wall Street Journal* with the straight forward title "On Behalf of Equifax, I'm Sorry." Barros expressed his "sincere and total apology to every consumer affected by our recent data breach" and confessed that "[w]e didn't live up to expectations." He also admitted that "we compounded the problem with insufficient support for consumers. Our website did not function as it should have, and our call center couldn't manage the volume of calls we received. Answers to key consumer

questions were too often delayed, incomplete or both. We know it's our job to earn back your trust."

160. On October 2, 2017, Equifax announced that it had revised its estimate of the number of people potentially affected by the Breach to a total of 145.5 million people, 2.5 million more than initially disclosed. Equifax released the new estimate after an assessment by Mandiant, which Equifax hired to perform a full review of the damage.

161. Subsequent to his resignation, Smith was forced to testify before the House of Representatives Energy and Commerce Committee. He outlined the events that led to the Breach, and said hackers were able to infiltrate a software weakness in an online portal that allows consumers to dispute items on their credit report. He also admitted that Equifax and other businesses that use the software had been warned of the vulnerability by the Department of Homeland Security's CERT on March 8, 2017.

162. Smith admitted: "We at Equifax clearly understood that the collection of American consumer information and data carries with it enormous responsibility to protect that data. We did not live up to that responsibility."

163. In testimony before Congress on October 3 and 4, 2017, Defendant Smith testified that one person at Equifax had the responsibility for notifying its

Information Technology team about the vulnerability and for instructing them to install the patch and that "the individual who was responsible for communicating to the organization to apply the patch did not." Moreover, Smith testified that "I am not certain that the individual who was responsible for communicating that the patch needed to be applied – that he knew the software was deployed." Smith's testimony is an admission that, contrary to basic data protection practices, Equifax failed to maintain an inventory of its security assets and did not build in any redundancies or checks. It is also an admission that neither he nor any of the Individual Defendants carried out their responsibility to monitor whether the patch had been installed.

164. Hearing Smith's testimony, one Congressman, Representative Greg Walden of Oregon, commented: "I don't think we can pass a law that, excuse me for saying this, fixes stupid. I can't fix stupid[ity]."

165. Smith's testimony that the responsibility for instructing the IT team to install the patch fell on a single individual drew severe criticism from cybersecurity experts. Professor Jamie Winterton, Director of Strategy at Arizona State University's Global Security Initiative, told the United States Senate in an October 11, 2017, submission:

> During the hearing, the former CEO of Equifax argued that the breach was in part due to "human error" – that an individual on the security team did not install a patch or communicate clearly which patch should be installed. I disagree. **This is not an error at the human level, but an error at a leadership and an organizational level. For a single individual to be responsible for Equifax's patch management shows an institutional lack of concern for security** and lack of respect for the people whose data they maintained.

(Emphasis added).

166. Similarly, George Hulme, an internationally recognized information security and business technology analyst, in an October 17, 2017 article in *Security Boulevard* entitled "No Mr. Equifax CEO You Don't Get To Blame One 'IT Guy' For Your Breach," wrote: "It's inconceivable that the CEO of any company – especially any company whose primary value rests with being a good steward of data – [would] blame the breach on bad assessments and communication." He explained:

> Security is a discipline of layered defenses and controls that all contribute to the adequate prevention, detection, and response to a data breach. Nearly every company will fail, to some degree, at prevention. **To have a breach of the magnitude Equifax has experienced one has to fail substantially at prevention, detection, and response.** A number of bad assessments and one IT person's error is ***not an acceptable reason to fail at data breach prevention, detection, and response – not a company that is actually trying to secure its assets with adequate security personnel, processes, and tools. And it's not a reason the world will accept, either***.

(Emphasis added).

167. Similarly, Amit Yoran was quoted in the October 30, 2017 edition of *Security Boulevard* as stating that reliance upon one person to secure Equifax's entire cyber infrastructure is "dumbfounding." He asked: "In what world does this seem like a reasonable standard of care??"

168. At an October 5, 2017 House Financial Services Committee hearing, Representative Carolyn Maloney pointed out that, in contrast to Equifax's inadequate manual patching process, Equifax's peers deployed a fully automated process that successfully detected and fixed the Apache Struts vulnerability. Experian, she said, has a patch management system that "will literally shut down [the vulnerable system automatically] if a patch isn't implemented immediately."

169. *The Atlanta Journal Constitution* reported on February 3, 2018 that "Equifax is the most hated company in America, according to a survey posted Jan. 22 on 247wallst.com."

170. As noted in a February 2018 Report entitled "Bad Credit: Uncovering Equifax's Failure to Protect Americans' Personal Information," prepared by the Office of Senator Elizabeth Warren after a four-month investigation, consumers who called the Equifax call center after the Breach had "hours-long waits," dropped calls, uncertain and incomplete responses, and agents not calling back as promised. A website set up by Equifax to help consumers determine whether their

data was compromised and how to protect themselves from the effects of the Breach had major vulnerabilities and technical flaws, making it "easy for others to impersonate and collect consumers' information." The site "asked consumers for some of the very same information that Equifax had already left vulnerable to hackers, including the last six digits of consumers' social security numbers."

171. It is clear that despite the importance of maintaining data security to Equifax's entire business, the Individual Defendants, in conscious disregard of and in breach of their fiduciary duties, caused or allowed Equifax to operate without adequate internal controls for preventing data breaches or quickly and effectively detecting and responding to them. Senator Warren's investigation revealed that Equifax's 150-page Corporate Crisis Management Plan (the "Crisis Plan") was deeply flawed. The Crisis Plan had not been updated since October 2014, even though the Individual Defendants knew that multiple cyberattacks had occurred since then, and it placed little emphasis on protecting the well-being of the millions of individuals whose data is used by Equifax, often giving short-shrift to the protection of consumer data.

172. The key overarching principles listed in the Crisis Plan are: "Place the highest priority on Life Safety. . . protect our assets and preserve our ability to operate and supply our customers, [and] maintain a strong Equifax reputation

through ethically and socially aware behaviors that ultimately preserve shareholder value." These key principles make no mention of protecting sensitive consumer data, which is the lifeblood of Equifax's business.

173. Further, the Crisis Plan's "Unauthorized Access Incident Handling Checklist" does not include a plan for informing consumers of potential access to their personal data even though that would be a reasonable and necessary procedure for a crisis plan. Even where informing affected consumers does appear in the Crisis Plan, the details of how and when to do so are vague and there is no strict timeline for informing consumers about a breach that places their personal data at risk. The Crisis Plan does require Equifax to notify affected consumers "in a clear and conspicuous manner, either by telephone or in writing" that their PII was compromised, but even that procedure was not followed.

174. After the Breach, Equifax only provided direct notice to 2.5 million of the 145.5 million affected consumers. The other affected consumers were forced to go to Equifax's post-breach website, which had significant technical issues and often directed them to phishing sites, to determine if they were affected and even then, consumers were required to submit partial social security numbers and the official response to consumers was often only that they "may" be affected.

175. Moreover, Equifax's haphazard response incurred consumer, regulator and political wrath because of lengthy wait times for customer service representatives and attempts to trick customers into enrolling for a credit monitoring service and waiving their right to sue in court. More specifically, Equifax supposedly offered "free" credit monitoring to those individuals affected by the Breach, but the offer's fine print included an arbitration clause and an automatic roll-over feature after one year that continued the credit monitoring with a fee. Thus, the Company's "cure" for the Individual Defendants' breaches of fiduciary duty was basically a way to limit Equifax's damages and one year later become a revenue source to the Company.

176. The Company has incurred significant damages as a result of the Individual Defendants' breaches of fiduciary duties in failing to maintain and implement adequate and reasonable measures to prevent, detect, and respond to cyberattacks. Among other losses, Equifax has lost contracts with major institutions, including The New York Times and the IRS due to the hacking scandal. The Company's CFO, Defendant Gamble, told securities analysts and investors at a June 13, 2018 William Blair Growth Stock Conference that:

> [R]ight after the cyber event occurred…most large customers, you'd probably go with virtually all great customers, put us in the penalty box…they indicated that no new business…no new contracts, no new

> products…there were products that would have been in negotiation that were about to sign contracts to start launching, that would have stopped.
>
> Gamble added: "What it means is, as you would have guessed, during the period when we couldn't engage with customers effectively, our competitors were very aggressive with those customers…. It's not lost on us that the two major competitors are performing extremely well." He also noted that it could take "18 to 24 months before things are kind of more normal." The Company also disclosed that Equifax is facing more than 240 Consumer Class Actions and more than 60 regulatory or governmental inquiries stemming from the Data Breach.

177. Equifax reported in its Form 10-Q, filed with the SEC on November 9, 2017, that extra spending on security and lawyers in the wake of the Breach helped push Equifax's third-quarter operating expenses to its highest on record. Breach related expenses cost the Company $87.5 million in the third quarter of 2017. The cost breakdown was as follows: $55.5 million in product costs, $17.1 million in professional fees, and $14.9 million in customer support costs. The Company also stated that it would be liable for the additional costs of free credit monitoring and identity theft protection it is offering all affected United States consumers. These additional costs are estimated between $56 and $110 million.

178. The Form 10-Q also noted that the Data Breach "has had a negative impact on our reputation" and:

> It is not possible to estimate the amount of loss or range of possible loss, if any, that might result from adverse judgments, settlements, penalties or other resolution of the above described proceedings and

> investigations based on the early stage of these proceedings and investigations, that alleged damages have not been specified, the uncertainty as to the certification of a class or classes and the size of any certified class, as applicable, and the lack of resolution on significant factual and legal issues.

179. Equifax's Form 10-K for the year ended December 31, 2017, discloses that the resolution of the lawsuits, claims, and government investigations "may result in damages, costs, fines or penalties substantially in excess of our insurance coverage, which, depending on the amount, could have a material adverse effect on our liquidity or compliance with our credit agreements."

180. During 2017 and 2018, Equifax is anticipated to incur $439 million of one-time costs, for which it has cyber insurance of $125 million. Approximately 50% of these costs are for incremental security data projects, 40% for legal and professional service fees, and 10% for free credit monitoring services. These costs do not include potential regulatory fines and penalties or legal judgments and settlements.

181. The 2017 Form 10-K and Annual Report also disclosed that the Company's revenue growth in 2017 "was negatively impacted by the cybersecurity incident. Certain of our customers have determined to defer or cancel new contracts or projects and others could consider such actions unless and until we can provide assurances regarding our ability to prevent unauthorized access to our

systems and the data we maintain. Many of our customers are requiring security audits of our systems . . . and any negative results of such audits may cause further losses of customers."

182. In addition certain of the Company's International Organization for Standardization ("ISO") certifications, which customer contracts and data suppliers require Equifax to maintain, have been suspended. These ISO certifications specify requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security system. "Due to the 2017 cybersecurity incident, certain of our ISO certifications have been suspended and we will be required to take additional remediation steps to retain such certifications, which efforts may not be successful."

183. Similarly, certain of the Company's payment card industry certifications have been suspended "which could result in fines and loss of access to data." In sum, "[i]f we are unable to demonstrate the security of our systems and the data we maintain and rebuild the trust of our customers, consumers and data suppliers, and if further negative publicity continues, we could experience a substantial negative impact on our business."

184. The 2017 Form 10-K and Annual Report also disclosed that: "Where we currently have exclusive use of data, the providers of the data sources could

elect to make the information available to competitors," which could have a "significant negative impact" on the Company's revenue, income and reputation.

185. On February 9, 2018, news broke that Equifax's fall 2017 disclosures regarding the scope of the Breach omitted key information. The Company submitted a document to the U.S. Senate Banking Committing stating that the hackers had also accessed passport numbers, tax identification numbers, email addresses, and drivers' license information from the affected individuals. With access to this more-complete scope of PII, it will be even easier for hackers to impersonate the 145.5 million affected Americans than previously thought.

186. In February 2018, Equifax began offering "Lock & Alert" protection to all consumers affected by the Breach "free for life." This new service has also been littered with issues. For instance, when attempting to sign up, many consumers are given error messages telling them that a phone call is required or that the service is down for 24-48 hours. Rather than doing everything possible to regain consumer trust, the Individual Defendants have allowed Equifax to continue to harm consumers.

187. Despite the seemingly generous offer of free credit protection following the Breach, the Individual Defendants have largely guided Equifax to use the Breach as a money-making opportunity at the expense of its victims. In the

immediate aftermath of the Breach, Equifax charged consumers the full amount legally allowed to freeze their credit, $30.95 per credit bureau. After widespread public outcry, the Company was forced to start offering free credit freezes, but that was only until its new "credit lock" product, Lock & Alert, was released in February 2018. Lock & Alert provides some of the same services as the former $30.95 product, but without the legal protections for consumers. Equifax controls this new product, which means it can control its features and can control whether it remains free after public outrage over the Breach subsides. When Equifax decides to end the free service, consumers will be forced to pay for a similar product to protect themselves or open themselves up to identity theft because of Equifax's malfeasance.

188. During defendant Smith's October 4, 2017 Senate hearing, Senator Warren observed, "So far, 7.5 million people have signed up for free credit monitoring through Equifax since the Breach. If just 1 million of them buy just one more year of monitoring through Equifax at the standard rate of $17 a month, that is more than $200 million in revenue for Equifax because of this breach."

189. To this end, in the aftermath of the Breach, many consumers became deeply concerned about their PII and enrolled in credit protection from LifeLock with LifeLock reporting a tenfold increase in enrollment during the month after the

Breach was made public. Defendant Smith confirmed under questioning from Senator Warren that LifeLock uses Equifax to monitor its customers' credit and pays Equifax a per-customer fee for the use of its services. Therefore, by allowing Equifax to have woefully inadequate security measures that resulted in the Breach, the Individual Defendants have created the sickness and now they are also selling the cure.

190. The size and breadth of the Breach has led lawmakers to propose legislation to curb future breaches. Senators Warren and Mark Warner of Virginia proposed the Data Breach Prevention and Compensation Act on February 7, 2018 (the "Proposed Act"). Pursuant to the Proposed Act, a company like Equifax that had its data breached would be liable for $100 to each consumer whose personal information was stolen and $50 for each additional piece of information compromised. It is estimated that under the Proposed Act, Equifax would owe over $1.5 billion for the Breach. The Proposed Act would not be retroactive, but would ensure that if another breach occurs in the future the financial consequences to Equifax will be astronomical.

191. On May 23, 2018, Moody's Investor Service issued a Global Credit Research report assigning a Baa1 rating to Equifax's $600 million of senior unsecured notes. Moody's explained that the rating "reflects the company's

challenges in managing the fallout of the security breach incident and its heightened regulatory and litigation risk over the next 2 to 3 years." The report added that: "We expect these challenges to weigh on Equifax's 2018 operating performance, resulting in a significant deceleration in revenue growth and erosion in adjusted EBITDA margins." The reduced rating increases Equifax's cost of borrowing.

192. On April 10, 2018, Bank of America/Merrill Lynch initiated coverage of Equifax with a report headlined "Equifax brand impaired: Initiate at Underperform."

G. THE INDIVIDUAL DEFENDANTS CAUSED EQUIFAX TO ISSUE MATERIALLY FALSE AND MISLEADING STATEMENTS

193. On February 24, 2016, the Individual Defendants caused Equifax to file a Form 10-K with the SEC, reporting the Company's financial and operating results for the fourth quarter and year ended December 31, 2015 ("2015 10-K"). The 2015 10-K was signed by defendants Smith, Gamble, Daleo, Driver, Feidler, Humann, Marcus, Marshall, McKinley, and Templeton. For the quarter, the Company reported revenue of $666.3 million, or $0.96 per share, an increase of 7% compared to the previous year. For the year, the Company reported revenue of $2.7 billion, or $3.55 per share, an increase of 9%.

194. In addition, the 2015 10-K described the Company's business strategy and, most notably, Equifax's claimed effort to invest in the security of its services:

> **OUR BUSINESS STRATEGY**
>
> Our strategic objective is to be the global leader in information solutions that creates unparalleled insights to solve customer challenges. Data is at the core of our value proposition. Leveraging our extensive resources, we deliver differentiated decisions through a broad and diverse set of data assets, sophisticated analytics and proprietary decisioning technology. Our long-term corporate growth strategy is driven by the following imperatives:
>
> - **Deliver consistently strong profitable growth and shareholder returns.** We seek to meet or exceed our financial commitments on revenue growth and margins through disciplined execution of our strategic initiatives and by positioning ourselves as a premier provider of high value information solutions.
>
> - **Develop unparalleled analytical insights leveraging Equifax unique data.** We continue to invest in and acquire unique sources of credit and non-credit information to enhance the variety and quality of our services while increasing clients' confidence in information-based business decisions. Areas of focus for investment in new sources of data include, among others, positive payment data, real estate data and new commercial business data. We also have developed unique capabilities to integrate customer and third-party data into our solution offerings to further enhance the decisioning solutions we develop for our customers.
>
> ***We continue to invest in and develop new technology to enhance the functionality, cost-effectiveness and security of the services we offer and further differentiate our products from those offered by our competitors***. In addition to custom products for large clients, we develop off-the-shelf, decisioning technology platforms that are more cost effective for medium and smaller-sized clients. We also develop predictive scores and analytics, some of which leverage multiple data

> assets, to help clients acquire new customers and manage their existing customer relationships. We develop a broad array of industry, risk management, cross-sell and account acquisition models to enhance the precision of our clients' decisioning activities. We also develop custom and generic solutions that enable customers to more effectively manage their debt collection and recovery portfolios.
>
> * * *
>
> • **Serve as a trusted steward and advocate for our customers and consumers.** This includes continuously improving the customer and consumer experience in our consumer and commercial offerings, anticipating and executing on regulatory initiatives***, while simultaneously delivering security for our services***.

(Emphasis added).

195. On February 22, 2017, the Individual Defendants caused Equifax to file the 2016 10-K with the SEC, reporting the Company's financial and operating results for the fourth quarter and year ended December 31, 2016. The 2016 10-K was signed by defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, and Templeton. For the quarter, the Company reported revenue of $801.1 million, or $1.01 per share, an increase of 20% compared to the previous year. For the year, the Company reported revenue of $3.1 billion, or $4.04 per share, an increase of 18%.

196. The 2016 10-K provided a similar description of the Company's business strategy and Equifax's claimed effort to invest in the security of its services:

OUR BUSINESS STRATEGY

Our strategic objective is to be the global leader in information solutions that creates unparalleled insights to solve customer challenges. Data is at the core of our value proposition. Leveraging our extensive resources, we deliver differentiated decisions through a broad and diverse set of data assets, sophisticated analytics and proprietary decisioning technology. Our long-term corporate growth strategy is driven by the following imperatives:

- **Deliver consistently strong profitable growth and shareholder returns**. We seek to meet or exceed our financial commitments on revenue growth and margins through disciplined execution of our strategic initiatives and by positioning ourselves as a premier provider of high value information solutions.

- **Develop unparalleled analytical insights leveraging Equifax unique data**. We continue to invest in and acquire unique sources of credit and non-credit information to enhance the variety and quality of our services while increasing clients' confidence in information-based business decisions. Areas of focus for investment in new sources of data include, among others, positive payment data, fraud and personal identification data, real estate data and new commercial business data. We also have developed unique capabilities to integrate customer and third-party data into our solution offerings to further enhance the decisioning solutions we develop for our customers.

We continue to invest in and develop new technology to enhance the functionality, cost-effectiveness and security of the services we offer and further differentiate our products from those offered by our competitors. In addition to custom products for large clients, we develop software as a service based, decisioning and data access technology platforms that are more cost effective for clients of all sizes. We also develop predictive scores and analytics, some of which leverage multiple data assets, to help clients acquire new customers and manage their existing customer relationships. We develop a broad array of industry, risk management, cross-sell and account acquisition models to enhance the precision of our clients' decisioning

> activities. We also develop custom and generic solutions that enable customers to more effectively manage their debt collection and recovery portfolios.
>
> * * *
>
> • **Serve as a trusted steward and advocate for our customers and consumers**. This includes continuously improving the customer and consumer experience in our consumer and commercial offerings, anticipating and executing on regulatory initiatives, ***while simultaneously delivering security for our services.***

(Emphasis added).

197. Interestingly, Equifax's 2017 Form 10-K, which was filed after the Data Breach was publicly disclosed, reverses the priority of the Company's business strategy "imperatives" by listing "**Serve as a trusted steward and advocate for our customers and consumers"** as the first imperative and adding to it that the Company uses "advanced security tools, techniques and processes in order to protect consumer specific information from fraudulent access" and delivering not merely "security for our services," but "industry leading security for our services."

198. On April 26, 2017, the Individual Defendants caused Equifax to issue a press release announcing the Company's financial and operating results for the first quarter ended March 31, 2017 ("Q1 2017 Press Release"). For the quarter, the

Company reported revenue of $832.2 million, or $1.26 per share, an increase of 14% compared to the previous year.

199. On April 27, 2017, the Individual Defendants caused Equifax to file a Form 10-Q with the SEC, reporting the Company's financial and operating results for the first quarter ended March 31, 2017 ("Q1 2017 10-Q"). In addition, Equifax disclosed an increase in capital expenditures which, among others purposes, served to improve "system reliability, security and disaster recovery enhancements." Specifically, the Company reported capital expenditures of $50.3 million, an increase of $10.1 million compared to the previous year. The Q1 2017 10-Q, discussing capital expenditures, states in relevant part:

> Our capital expenditures are used for developing, enhancing and deploying new and existing software in support of our expanding product set, replacing or adding facilities and equipment, updating systems for regulatory compliance, the licensing of software applications and investing in system reliability, security and disaster recovery enhancements. Capital expenditures in the first three months of 2017 increased by $10.1 million from the same period in 2016 as we paid amounts that were accrued as of December 31, 2016.

200. On July 26, 2017, the Individual Defendants caused Equifax to issue a press release announcing the Company's financial and operating results for the second quarter ended June 30, 2017 ("Q2 2017 Press Release"). For the quarter, the Company reported revenue of $856.7 million, or $1.36 per share, an increase of

6% compared to the previous year. The Company highlighted strong revenue growth driven by Equifax's identity and fraud solutions, stating in relevant part:

Strong Execution, Revenue Growth and Margin Expansion Drive Double-Digit EPS growth

- Revenue of $856.7 million was up 6 percent (7 percent in local currency) compared to the second quarter of 2016.

- Diluted EPS of $1.36 was up 26 percent compared to the second quarter of 2016.

- Adjusted EPS of $1.60 was up 12 percent compared to the second quarter of 2016.

- Net income attributable to Equifax of $165.4 million was up 26 percent compared to the second quarter of 2016.

- Adjusted EBITDA margin was 39.1 percent compared to 36.6 percent in the second quarter of 2016.

ATLANTA, July 26, 2017 -- Equifax Inc. (NYSE: EFX) today announced financial results for the quarter ended June 30, 2017.

"***Second quarter performance reflects outstanding execution by the team*** and the strength of our unique portfolio of businesses," said Richard F. Smith, Chairman and Chief Executive Officer at Equifax. "The team continues to make significant progress on new product innovation and our enterprise growth initiatives, both in the U.S. and around the world. We remain confident in our outlook for 2017 and are optimistic about the opportunities in front of us as we look ahead to 2018."

Financial Results Summary

The company reported revenue of $856.7 million in the second quarter of 2017, a 6 percent increase compared to the second quarter of 2016 on a reported basis and up 7 percent on a local currency basis.

Second quarter diluted EPS attributable to Equifax was $1.36, up 26 percent compared to the second quarter of 2016. Adjusted EPS attributable to Equifax was $1.60, up 12 percent compared to the second quarter of 2016. This financial measure for 2017 excludes the income tax effects of stock awards recognized upon vesting or settlement and for 2016 excludes Veda acquisition related amounts. The financial measure for both 2017 and 2016 excludes acquisition-related amortization expense, net of associated tax impacts. These items are described more fully in the attached Q&A.

Net income attributable to Equifax of $165.4 million was up 26 percent compared to the second quarter of 2016. Adjusted EBITDA margin was 39.1 percent, compared to 36.6 percent in the second quarter of 2016. These financial measures for 2017 and 2016 have been adjusted for certain items, which affect the comparability of the underlying operational performance and are described more fully in the attached Q&A.

USIS delivered strong revenue growth driven by mortgage, marketing and analytic services, and identity and fraud solutions.

- Total revenue was $331.9 million in the second quarter of 2017 compared to $307.9 million in the second quarter of 2016, an increase of 8 percent. Operating margin for USIS was 45.1 percent in the second quarter of 2017 compared to 43.5 percent in the second quarter of 2016. Adjusted EBITDA margin for USIS was 51.5 percent in the second quarter of 2017 compared to 50.4 percent in the second quarter of 2016.

- Online Information Solutions revenue was $232.6 million, up 6 percent compared to the second quarter of 2016.

- Mortgage Solutions revenue was $38.6 million, up 10 percent compared to the second quarter of 2016.

- Financial Marketing Services revenue was $60.7 million, up 15 percent compared to the second quarter of 2016.

* * *

Third Quarter 2017 and Full Year 2017 Outlook

We are off to a strong start through the first half of 2017. For the third quarter, at current exchange rates, we expect revenue to be between $853 and $861 million, reflecting growth of 6-7%, with limited foreign exchange impact. Adjusted EPS is expected to be between $1.50 and $1.54 which is up 4% to 7%, also with limited foreign exchange impact.

We expect full year 2017 revenue to be between $3.395 and $3.425 billion, reflecting constant currency growth of approximately 9%. Adjusted EPS for the year is expected to be between $6.02 and $6.10, which is up approximately 10%.

(Emphasis added).

201. On July 27, 2017, the Individual Defendants caused Equifax to file a Form 10-Q with the SEC, reporting the Company's financial and operating results for the second quarter ended June 30, 2017 ("Q2 2017 10-Q"). As initially disclosed in the Q2 2017 Press Release, Equifax reported an increase in capital expenditures. For the first and second quarters of 2017, the Company reported capital expenditures of $99.9 million, an increase of $17.1 million compared to 2016. The Q2 2017 10-Q stated in relevant part:

> Our capital expenditures are used for developing, enhancing and deploying new and existing software in support of our expanding product set, replacing or adding facilities and equipment, updating systems for regulatory compliance, the licensing of software applications and investing in system reliability, security and disaster recovery enhancements. Capital expenditures in the first six months of 2017 increased by $17.1 million from the same period in 2016 as we paid amounts that were accrued as of December 31, 2016.

202. On August 16, 2017, more than two weeks after Equifax discovered the Breach and after defendant Smith had definitively learned that a massive amount of PII had been stolen, Equifax held an investor presentation discussing the state of the Company and plans for the future. The presentation completely neglected to mention the Breach.

203. The statements in paragraphs 194, 196, 200, and 201 above were materially false and/or misleading because they misrepresented and failed to disclose material, adverse facts pertaining to the Company's business, operations, and prospects, which were known to the Individual Defendants or recklessly disregarded by them. Specifically, the Individual Defendants made false and/or misleading statements and/or failed to disclose that: (a) Equifax failed to develop, implement, and maintain adequate and necessary measures to safeguard and protect its data systems; (b) Equifax ignored and failed to comply with repeated warnings and explicit instructions to promptly patch its software; (c) Equifax failed to develop, implement, and maintain adequate monitoring systems to detect

security breaches; (d) Equifax failed to develop, implement, and maintain proper data security systems, controls, and monitoring systems; (e) Equifax failed to develop, implement, and maintain adequate and reasonable measures to respond to known risks concerning its data security systems, controls, and monitoring systems; (f) Equifax inadequately assessed the risks associated with the Company's data security; (g) Equifax failed to maintain effective internal controls over financial reporting; (h) Equifax lacked a crisis management plan to respond quickly, effectively, and sufficiently to a major data breach; and (as a result of the foregoing, Equifax's public statements, made or caused to be made by the Individual Defendants, were materially false and misleading, omitted material facts, and/or lacked a reasonable basis at all relevant times.

1. Defendants Gamble, Loughran, Ploder and Brandberg Unlawfully Profited at Equifax's Expense by Selling Shares at Artificially-Inflated Prices

204. While the false statements described above harmed public investors and shareholders, defendants Gamble, Loughran, Ploder and Brandberg sold significant amounts of their personal Equifax holdings at artificially-inflated prices prior to the public disclosure of the Breach.

205. Defendant Gamble is Equifax's CFO and Corporate Vice President. Gamble has held these roles since May 2014. Gamble was aware of material,

adverse, and non-public information regarding Equifax's cybersecurity deficiencies and the Company's statements related thereto. While in possession of this information, Gamble sold at least 20,500 shares of Equifax stock (almost one-third of his holdings), at artificially-inflated prices, for total proceeds of $2,856,506, as follows: (a) on May 23, 2017, Gamble sold 14,000 shares at $136.438 per share for proceeds of $1,910,132; and (b) on August 1, 2017, Gamble sold 6,500 shares at $145.596 per share for proceeds of $946,374.

206. Defendant Loughran is President of Equifax's USIS unit. Loughran has worked for the Company since March 2006. Loughran was aware of material, adverse, and non-public information regarding Equifax's cybersecurity deficiencies and the Company's statements related thereto. On August 1, 2017, while in possession of this information, Loughran sold at least 4,000 shares of Equifax stock at the artificially-inflated price of $146.02 per share for proceeds of approximately $584,098.80.

207. Defendant Ploder is Equifax's President of Workforce Solutions. Ploder has held that role since November 2014. Ploder was aware of material, adverse, and non-public information regarding Equifax's cybersecurity shortcomings and the Company's statements related thereto. On August 1, 2017,

while in possession of this information, Ploder sold 1,719 shares of Equifax stock at the artificially-inflated price of $145.70 per share for proceeds of $250,458.30.

208. Defendant Brandberg is Equifax's Senior Vice President, Investor Relations. Brandberg was aware of material, adverse, and non-public information regarding Equifax's cybersecurity shortcomings and the Company's statements related thereto. On August 1, 2017, while in possession of this information, Brandberg sold 1,724 shares of Equifax stock at artificially-inflated prices for proceeds of more than $250,000.

209. These insider sales were all executed while Equifax's stock price was artificially inflated due to the unlawful conduct and the misrepresentations and omissions alleged herein, including the Individual Defendants' knowledge of the Data Breach and awareness that the Company was being operated in a manner that made it highly susceptible to committing the precise unlawful conduct alleged herein, and the Individual Defendants' failure to prevent the same by ensuring that the Company implemented and maintained reasonably adequate data security measures to safeguard and protect consumers' personal data.

210. The shares sold by defendants Gamble, Loughran, Ploder, and Brandberg totaling more than $2 million in proceeds took place 40 days before the

Breach was disclosed to the public. These transactions were not part of any 10b5-1 trading plan.

211. Because of their roles as directors and/or officers of Equifax, defendants Gamble, Loughran, Ploder, and Brandberg either knew, consciously disregarded, were reckless and grossly negligent in not knowing, or should have known material, adverse, and non-public information about the Company's business practices, operations, financials, compliance policies and practices, and internal controls, including, *inter alia*, that the unlawful conduct and the false and misleading statements alleged herein, as well as the material omissions from those statements, caused the price of the Company's stock to trade at artificially-inflated prices at the same time they were disposing of millions of dollars' worth of Company stock. Defendants Gamble, Loughran, Ploder and Brandberg had a duty to refrain from selling Equifax shares while in possession of material, adverse, non-public information concerning Equifax's business practices, operations, financials, compliance policies and practices, and internal controls, but they violated this duty and in doing so, were able to achieve a financial benefit not shared by Equifax's other shareholders in violation of their fiduciary duties and the federal securities laws.

212. After the Breach became public and amid public outrage regarding the insider sales, the Director Defendants formed a Special Committee, comprised of defendants Daleo, Hough, and Stock, to investigate the insider sales.

213. On November 3, 2017, the Special Committee determined that Gamble, Equifax's CFO, "did not have any knowledge of the security incident when he sought preclearance to trade on July 31 or when he executed his cleared trades on August 1." The Committee further determined that Gamble did not learn of the Breach affecting 145.5 million consumers until "August 10, during a management office meeting" almost two weeks after Equifax discovered it. This is simply not credible given Gamble's position as a senior executive officer and that the Breach was the most severe data breach in American history.

214. The Special Committee made similar findings regarding Loughran, Ploder, and Brandberg, determining that they did not learn about the Breach until mid-August 2017.

215. The Special Committee's determinations are not credible in light of the coordinated sale of substantial inside holdings by several executives on the same day just ahead of the disclosure of materially, adverse information. Moreover, the credibility of the Special Committee's investigation is substantially undermined by the fact that, though unmentioned by the Special Committee,

Gamble, Loughran, Ploder and Brandberg were not the only Equifax insiders to profit through insider stock sales from the concealment of the Data Breach. Notwithstanding dozens of interviews and the review of more than 55,000 documents in an investigation that covered "all officers of the company," the Special Committee failed to detect that the Chief Information Officer for Equifax's U.S Information Solutions Business, Jun Ying ("Ying"), who was next in line to become the Company's Chief Information Officer, sold $950,000 worth of Equifax stock before public disclosure of the Data Breach. Ying has been criminally charged by the SEC with insider trading. The Special Committee also failed to detect admitted insider trading related to the Breach by former Equifax software development manager Sudhakar Reddy Bonthu ("Bonthu"), casting serious doubt on the thoroughness of the Special Committee's investigation.

216. The DOJ has opened a criminal investigation into the suspiciously timed sales and the SEC is also conducting a similar investigation. On March 14, 2018, the Department of Justice announced that Ying had been indicted for insider trading. The press release disclosed that on Friday, August 25, 2017, Ying texted a co-worker that the breach they were working on "Sounds bad. We may be the one breached." The following Monday, Ying conducted web searches on the impact of Experian's 2015 data breach on its stock price. Later that morning, Ying exercised

all of his available stock options, which he then sold. "This defendant took advantage of his position as Equifax's USIS Chief Information Officer and allegedly sold over $950,000 worth of stock to profit before the company announced a data breach that impacted over 145 million Americans," said U.S. Attorney Byung J. Pak. "Our office takes the abuse of trust inherent in insider trading very seriously and will prosecute those who seek to profit in this manner." David J. LeValley, Special Agent in Charge of FBI Atlanta, added: "The alleged actions of this defendant undermine the public's confidence in the nation's stock markets. By prosecuting cases like this, the FBI and the U.S. Securities and Exchange Commission are sending a strong message to company insiders that they must follow the same rules that govern regular investors. Otherwise, they face the severe consequences for failing to do so."

217. Moreover, the Special Committee limited its document review to the period beginning July 29, 2017. Notwithstanding the insider status of these defendants and the Breach having been the most severe data breach in American history, the Special Committee did not review documents generated between March 7, 2017 and July 28, 2017, when the warnings, alerts and instructions were first provided to Equifax and the Data Breach was taking place. There is also no

mention in the report of the Special Committee reviewing external brokerage records of senior officers and directors.

218. On June 4, 2018, *The Wall Street Journal* noted: "The report clearing the Equifax executives likely won't prompt the SEC to drop its investigation of their share sales, some securities law specialists said. And despite the exoneration, government securities regulators could still find 'problematic activity related to the stock sales,' said Charles Elson, a securities law specialist and head of the Weinberg Center for Corporate Governance at University of Delaware."

219. On June 28, 2018, the SEC announced that Bonthu was charged with insider trading. In a complaint filed in federal court in Atlanta, the SEC charged that Bonthu traded on confidential information he received while creating a website for consumers impacted by the Data Breach. According to the complaint, Bonthu was told the work was being done for an unnamed potential client, but based on information he received, he concluded that Equifax itself was the victim of the breach. The SEC alleges that Bonthu violated company policy when he traded on the non-public information by purchasing Equifax put options. Less than one week later, after Equifax publicly announced the Data Breach, Bonthu sold the put options. "As we allege, Bonthu, who was entrusted with confidential information by his employer, misused that information to conclude that his

company had suffered a massive data breach and then sought to illegally profit," said Richard R. Best, Director of the SEC's Atlanta Regional Office. In a parallel proceeding, the U.S. Attorney's Office for the Northern District of Georgia filed criminal charges against Bonthu.

220. On July 3, 2018, it was reported that Bonthu settled the SEC's suit, admitted to capitalizing on undisclosed information regarding the Data Breach, and agreed to forfeit more than $75,000 in ill-gotten gains in a consent agreement filed in this Court. According to the consent order, Bonthu has agreed to plead guilty in the criminal case. The consent agreement reflects yet again an egregious failure by Equifax and the Individual Defendants regarding the Data Breach. According to the consent agreement, Bonthu was asked to assist in responding to the breach on August 25, 2017, without being told Equifax was the target. This attempt at maintaining secrecy was entirely negated by the fact that a work-related email Bonthu received the next day relating to work on the cyber intrusion had a file attached labeled "EFXDatabreach.postman_collection." Equifax's stock ticker symbol is "EFX" and this email plainly revealed that Equifax was the target of the cyber-attack, affording Bonthu the opportunity, of which he availed himself, to profit through the Individual Defendants' failure to timely disclose the Data Breach.

2. The Director Defendants Caused Equifax to Repurchase Stock Despite Knowing That Critical Company Data Protection Systems Were Either Non-Existent or Defective and That They Were Not Monitoring Compliance With Warnings and Instructions

221. While Equifax's shares were trading at artificially-inflated prices because of the Individual Defendants' material misrepresentations and omissions concerning the Company's operations and financial and business prospects as alleged above, the Director Defendants caused the Company to repurchase millions of dollars' of its common stock at inflated prices using Company funds.

222. During July and August 2017, with full knowledge that Equifax lacked proper security controls to protect the privacy of the millions of consumers whose data it housed, the Director Defendants caused the Company to repurchase 535,901 common shares of Equifax on the open market – a stark departure from the Company's prior pattern of stock repurchases. The Company had not repurchased shares as part of its stock repurchase program in 2016 or in the first or second quarters of 2017.

223. On November 9, 2017, the Individual Defendants caused Equifax to file a Form 10-Q with the SEC, reporting that between July 1, 2017 and August 31, 2017, the Company repurchased 535,901 shares, at an average price of $143.88 per share, for a total of over $77 million. By September 15, 2017, one week after the

Company disclosed the Breach to the public, the value of this stock had declined to approximately $49.8 million, or over 35%, resulting in a loss of over $27.2 million for the Company.

224. Despite the Director Defendants' knowledge of the numerous warnings, alerts, and instructions to patch software, their knowledge that they had failed to monitor whether the patch had been applied, and their knowledge that Equifax had the "Most Inherent Risk Profile" of a disastrous cyber-attack, the Director Defendants authorized and executed Equifax's share repurchases at artificially-inflated prices. Indeed, the Individual Defendants knew, for a portion of the period for which they were executing stock buy-backs, that Equifax stock was artificially inflated because they knew that the Data Breach had occurred, its massive scale, and that the facts had not been publicly disclosed. The Director Defendants' decisions to repurchase were not the product of a valid business judgment because they knew at the time of repurchase that the Company's stock was significantly inflated due to the false and misleading statements and omissions set forth herein.

225. By approving the stock repurchases at a time when Equifax's stock price was artificially inflated, the Director Defendants breached their fiduciary duties by causing the Company to waste corporate assets.

3. The Director Defendants Caused Equifax to Issue False or Misleading Statements Regarding Data Security as they Approved Massive Share Repurchases

226. On February 22, 2017, the Individual Defendants caused Equifax to file the 2016 10-K with the SEC reporting revenue of $801.1 million (or $1.01 per share) for the fourth quarter of 2016, an increase of 20% compared to 2015. The 2016 10-K also reported annual revenue of $3.1 billion (or $4.04 per share), an increase of 18%. Lastly, the 2016 10-K stated that Equifax's disclosure controls and procedures were effective as of December 31, 2016. The 2016 10-K expounded on this topic as follows:

> *Security breaches and other disruptions to our information technology infrastructure could interfere with our operations, and could compromise Company, customer and consumer information, exposing us to liability which could cause our business and reputation to suffer.*
>
> In the ordinary course of business, we rely upon information technology networks and systems, some of which are managed by third parties, to process, transmit and store electronic information, and to manage or support a variety of business processes and activities, including business-to-business and business-to-consumer electronic commerce and internal accounting and financial reporting systems. Additionally, we collect and store sensitive data, including intellectual property, proprietary business information and personally identifiable information of our customers, employees, consumers and suppliers, in data centers and on information technology networks. The secure and uninterrupted operation of these networks and systems, and of the processing and maintenance of this information, is critical to our business operations and strategy.

> Despite our substantial investment in physical and technological security measures, employee training, contractual precautions and business continuity plans, our information technology networks and infrastructure or those of our third-party vendors and other service providers could be vulnerable to damage, disruptions, shutdowns, or breaches of confidential information due to criminal conduct, denial of service or other advanced persistent attacks by hackers, employee or insider error or malfeasance, or other disruptions during the process of upgrading or replacing computer software or hardware, power outages, computer viruses, telecommunication or utility failures or natural disasters or other catastrophic events. Unauthorized access to data files or our information technology systems and applications could result in inappropriate use, change or disclosure of sensitive and/or personal data of our customers, employees, consumers and suppliers.
>
> We are regularly the target of attempted cyber and other security threats and must continuously monitor and develop our information technology networks and infrastructure to prevent, detect, address and mitigate the risk of unauthorized access, misuse, computer viruses and other events that could have a security impact. Insider or employee cyber and security threats are increasingly a concern for all large companies, including ours. Although **we are not aware of any material breach of our data, properties, networks or systems**, if one or more of such events occur, this potentially could compromise our networks and the information stored there could be accessed, publicly disclosed, lost or stolen. Any such access, disclosure or other loss of information could subject us to litigation, regulatory fines, penalties or reputational damage, any of which could have a material effect on our cash flows, competitive position, financial condition or results of operations. Our property and business interruption insurance may not be adequate to compensate us for all losses or failures that may occur. Also, our third-party insurance coverage will vary from time to time in both type and amount depending on availability, cost and our decisions with respect to risk retention.

(Emphasis added).

227. The representation in the 2016 10-K that "we are not aware of any material breach of our data, properties, networks or systems," was materially false and misleading because the Individual Defendants were aware of a series of breaches of Equifax's systems in 2016 and prior years, as discussed in Section IX E herein.

228. The 2016 10-K was signed by defendants Smith, Gamble, Daleo, Driver, Feidler, Hough Humann, Marcus, Marshall, McKinley, Stock, and Templeton, and certified pursuant to the Sarbanes-Oxley Act of 2002 ("SOX") by defendants Smith (as CEO and Chairman) and Gamble (as CFO) as follows:

> 1. I have reviewed this annual report on Form 10-K of Equifax Inc.;
>
> 2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;
>
> 3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;
>
> 4. The registrant's other certifying officer(s) and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as

defined in Exchange Act Rules 13a-15(f) and 15(d)-15(f)) for the registrant and have:

a) Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

b) Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

c) Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

d) Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and

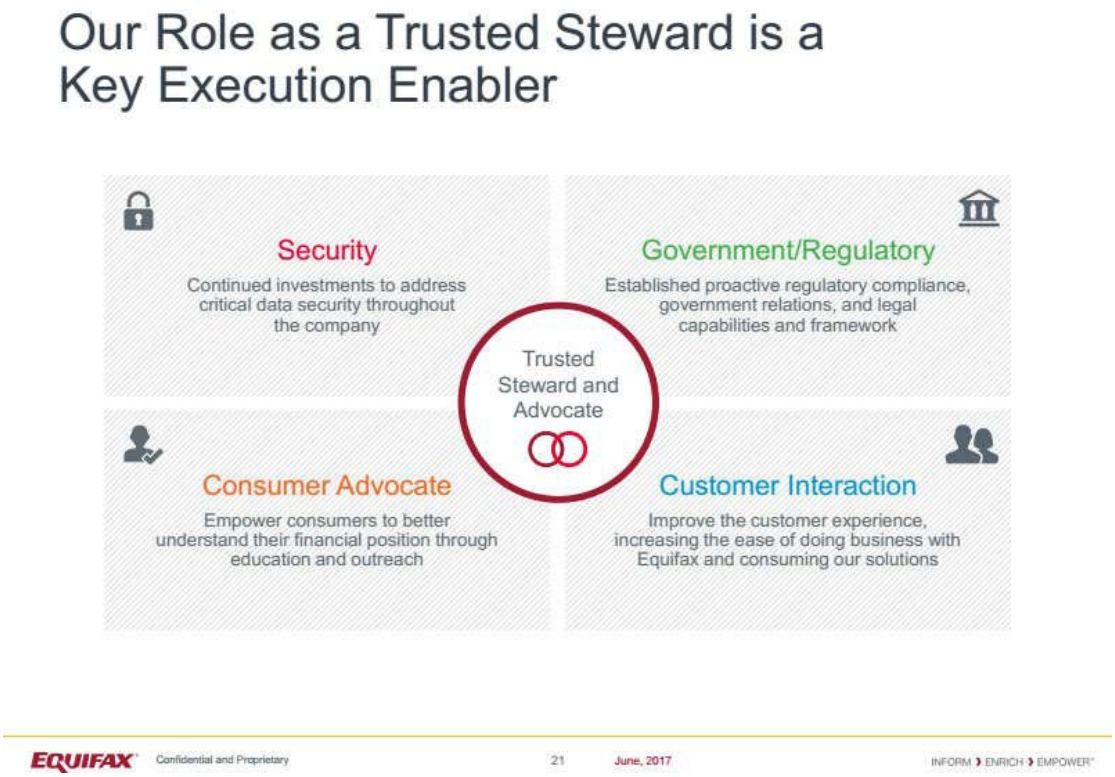
5. The registrant's other certifying officer(s) and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):

a) All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and

b) Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

229. On April 26 and 27, 2017, the Individual Defendants caused Equifax to issue and file the Q1 2017 Press Release and Q1 2017 10-Q, respectively, as described in paragraphs 198 and 199 above. The Q1 2017 10-Q was signed and certified pursuant to SOX by defendants Smith and Gamble. The SOX certification was substantially similar to that reproduced in the preceding paragraph.

230. On June 1, 2017, more than two months after being warned and instructed to apply the software patch and failing to do so, the Individual Defendants caused Equifax to hold an investor presentation, which touted the Company's data security as follows:



231. On June 7, 2017, at a Stephens Investor Conference, defendant Gamble boasted that Equifax's Workforce Solutions Segment, which had grown substantially over the previous five years, was driven in part by the Company's information exchange service, which "***provides a secure verification network*** where the contributors, as an employer contributes information into our exchange, ***we make sure that the people accessing that information have a right to see it***." (Emphasis added).

232. On July 26 and 27, 2017, the Individual Defendants caused Equifax to issue and file the Q2 2017 Press Release and Q2 2017 10-Q, respectively, as

described in paragraphs 200 and 201 above. The Q2 2017 10-Q was signed and certified pursuant to SOX by defendants Smith and Gamble. The SOX certification was substantially similar to that reproduced in paragraph 228 above.

233. On August 16, 2017, the Individual Defendants caused Equifax to hold another investor presentation, which touted the Company's data security using a slide identical to the June 1, 2017 investor presentation.

234. Defendant Smith also repeatedly discussed data security during his August 1, 2017 Terry College speech. He described the issue of data security for a large database like Equifax's as follows: "When you have the size database we have, it's very attractive for others to try to get into our database, [s]o it is a huge priority for us." During the speech, Smith was also asked specifically about data fraud and security and answered, "Fraud is a huge opportunity for us. It is a massive, growing business for us."

235. The statements referenced above in paragraphs 226 to 234 were materially false and misleading. The Individual Defendants caused Equifax to make, and/or personally made, the false and/or misleading statements, as well as failed to disclose material adverse facts regarding the Company's business practices, operations, financials, compliance policies and practices, and internal controls. Specifically, the Individual Defendants made, or caused the Company to

make, false and/or misleading statements, and/or failed to disclose that: (a) the Company failed to develop, implement, and maintain adequate measures to safeguard and protect its data systems; (b) the Company failed to develop, implement, and maintain adequate monitoring systems to detect security breaches; (c) the Company failed to develop, implement, and maintain proper data security systems, controls, and monitoring systems; (d) the Company failed to develop, implement, and maintain adequate measures to respond to known risks concerning its data security systems, controls, and monitoring systems; (e) the Company inadequately assessed the risks associated with the Company's data security; (f) the Company ignored and failed to comply with repeated warnings and instructions to promptly patch its software; (g) the Company failed to maintain effective internal controls over financial reporting; (h) the Company lacked a plan to quickly, effectively, and sufficiently respond to a major data breach; (i) the Company had, in fact, been a victim of the massive Data Breach; and (i) as a result of the foregoing, Equifax's public statements, made or caused to be made by the Individual Defendants, were materially false and misleading, omitted material facts, and/or lacked a reasonable basis at all relevant times. As a result of this fraud, the Individual Defendants were able to artificially inflate the Company's financials, and its stock price.

4. Equifax Relied on the Director Defendants' False and Misleading Statements When Repurchasing Stock

236. Equifax relied on the false or misleading statements of the Director Defendants, either directly or through the "fraud on the market" doctrine when repurchasing shares as described above.

237. At all relevant times, the market for Equifax common stock was an efficient market. Equifax stock met the requirements for listing, and was listed and actively traded on the NYSE, a highly efficient and automated market. According to Equifax's November 9, 2017 Form 10-Q, the Company had more than 120 million shares outstanding as of September 30, 2017. Hundreds of thousands of shares of Equifax stock are traded on a daily basis, demonstrating a very active and broad market for Equifax stock, and permitting a very strong presumption of an efficient market. Moreover, Equifax claims to be qualified to file a less comprehensive Form S-3 registration statement with the SEC that is reserved, by definition, to well-established and largely capitalized issuers for whom less scrutiny is required.

238. As a regulated issuer, Equifax filed periodic public reports with the SEC and NYSE. Equifax regularly communicated with public investors via established market communication mechanisms, including through regular dissemination of press releases on the national circuits of major newswire services

and through other wide-ranging public disclosures, such as communications with the financial press and other similar reporting services. Furthermore, Equifax was tracked by several securities analysts employed by major brokerage firms who wrote reports which were distributed to the sales force and certain customers of their respective brokerage firms. Each of these reports was publicly available and entered the public marketplace.

239. As a result of the foregoing, the market for Equifax common stock promptly digested current information regarding Equifax from all publicly available sources and reflected such information in the price of Equifax common stock. Under these circumstances, all purchasers of Equifax common stock suffered similar injury through their purchase of Equifax common stock at artificially-inflated prices, and a presumption of reliance thus applies.

240. Had Equifax known of the material adverse information not disclosed by the Individual Defendants, or had Equifax been aware of the truth behind the material misstatements of the Director Defendants, the Company would not have repurchased Equifax stock at the artificially-inflated prices. The Individual Defendants breached their fiduciary duties by causing or allowing these repurchases.

5. Neither the Statutory "Safe Harbor" Nor the "Bespeaks Caution" Doctrine Applies to the Individual Defendants' Misrepresentations

241. Neither the safe-harbor provision of the Private Securities Litigation Reform Act of 1995 (the "PSLRA") nor the judicially created "bespeaks caution" doctrine applicable to forward-looking statements under certain circumstances applies to any of the false or misleading statements pleaded herein. None of the subject statements constituted a forward-looking statement; rather, they were historical statements or statements or omissions of purportedly current facts and conditions at the time the statements were made, including statements about Equifax's data security controls and systems, its present financial condition, and its internal controls, among other things.

242. Alternatively, to the extent any of the false or misleading statements pleaded herein could be construed as forward-looking statements, they were not accompanied by any meaningful, cautionary language identifying important facts that could cause actual results to differ materially from those in the purportedly forward-looking statements. Further, to the extent the PSLRA's safe harbor would otherwise apply to any forward-looking statements pleaded herein, the Individual Defendants are liable for those false or misleading statements because, at the time each of those statements was made, the speaker(s) knew the statement was false

and misleading or omitted material facts, or the statement was authorized or approved by an executive of Equifax or an Individual Defendant who knew the statement was materially false or misleading or omitted material facts when made.

6. The Group Pleading Doctrine Applies to the Individual Defendants' Misstatements and Omissions

243. Lead Plaintiffs' claims against the Individual Defendants primarily allege that the Individual Defendants are liable because of information they received and decisions they made collectively. There is nothing to be gained by addressing each Individual Defendant individually because they are all similarly situated.

244. While defendant signatories, certifiers, or speakers are identified with respect to the false or misleading statements identified above, the group pleading doctrine also applies to render the Individual Defendants responsible for statements as to which they are not explicitly identified as the speaker, certifier, or signatory. The Individual Defendants participated in the drafting, preparation, or approval of the various shareholder and investor reports and other communications concerning Equifax identified herein, and were aware of or recklessly disregarded the misstatements contained in those reports and other communications as well as the omissions from them, and were aware of their materially false and misleading nature. Each Individual Defendant, by virtue of his or her position(s) at Equifax,

had access to adverse undisclosed information about the Company's business prospects and financial condition and performance as alleged herein, and knew or recklessly disregarded that those adverse facts rendered the subject statements materially false or misleading when made.

7. The Director Defendants' Misstatements and Omissions Damaged Equifax

245. In the wake of Equifax's disclosure of the Breach, the Company's stock price tumbled $19.49 per share (or approximately 13.7%), on unusually high trading volume, to close at $123.23 per share on September 8, 2017, resulting in a loss of approximately $2.34 billion in market capitalization. In the days that followed, the stock continued declining, reaching a low of $92.98 per share at closing on September 15, 2017 (eight days after the Breach was disclosed), representing a decline of $49.74 (or approximately 34.9%) per share, and a loss of approximately $6 billion in market capitalization.

246. The decline in Equifax's share price was a direct result of the nature and extent of the Director Defendants' wrongful conduct finally being revealed to the market. The timing and magnitude of the decline in the Company's share price negates any inference that the losses suffered by Equifax were caused by changed market conditions, macroeconomic or industry factors, or Company-specific facts unrelated to the Individual Defendants' wrongful conduct.

X. DERIVATIVE AND DEMAND ALLEGATIONS

247. Lead Plaintiffs bring this action derivatively in the right and for the benefit of Equifax to redress injuries suffered, and to be suffered, by Equifax as a direct result of breaches of fiduciary duties, violations of the federal securities laws, violations of consumer laws, waste of corporate assets, and unjust enrichment, as well as the aiding and abetting thereof, by the Individual Defendants. Equifax is named as nominal defendant solely in a derivative capacity.

248. Lead Plaintiffs will adequately and fairly represent the interests of Equifax in enforcing and prosecuting its rights.

249. On January 10, 2018, in accordance with O.C.G.A. § 14-2-742, the Weyl Plaintiffs made a demand on the Board to commence an action against the Individual Defendants (the "Weyl Demand") for the wrongdoing alleged herein. Other Equifax shareholders made similar demands.

250. In response to the Weyl Demand and the Demands of other Equifax shareholders, the Board of Directors formed a Demand Review Committee consisting of defendants Stock and Hough, the members of the Special Committee who conducted the insider trading investigation, to investigate and report on the Demands. The investigation being performed by the Demand Review Committee

cannot possibly pass the scrutiny of this Court because its members are not independent nor disinterested and its investigation cannot be in good faith.

251. As an initial matter, defendants Stock and Hough were members of the Technology Committee, whose responsibilities under the Technology Committee charter included, among other things, "review[ing] and monitor[ing] the Company's technology strategy and significant technology investments in support of its evolving global business needs" with their "[a]reas of review" including "information technology strategy" and the "Company's response to external technology-based threats and opportunities." In addition, the Technology Committee charter provided that the members of the Technology Committee "will oversee the Company's mitigation of any identified enterprise-wide risks in the above areas."

252. Given their heightened duties as members of the Technology Committee, which conferred upon Stock and Hough the prime responsibility for overseeing and monitoring cybersecurity at Equifax and preventing, detecting and responding to cyber-attacks, Stock and Hough are directly responsible for the misconduct alleged in the Demands such that the Demand Review Committee's conclusion can be given no deference. Having failed to provide timely and adequate risk oversight over a material enterprise risk despite numerous warnings;

having failed for months to monitor whether the warnings and instructions to apply the patch were heeded; and having failed to develop a comprehensive crisis management plan in the wake of the Breach, defendants Stock and Hough have a palpable self-interest, face a substantial likelihood of liability, are not independent and are in no position to fairly and impartially investigate the Demands and report thereon.

253. Moreover, as alleged herein, Stock and Hough, as members of the Special Committee, were tasked with investigating the insider selling at Equifax. They cleared defendants Gamble, Loughran, Ploder, and Brandberg of wrongdoing, but failed to detect that the Chief Information Officer for Equifax's U.S Information Solutions Business, Jun Ying, who was next in line to become the Company's Chief Information Officer, sold $950,000 of Equifax stock before disclosure of the Data Breach. Ying has been criminally charged by the SEC with insider trading. On June 28, 2018, it was also reported that former Equifax software development manager Sudhakar Reddy Bonthu was charged with insider trading related to the Breach. Both of these incidents cast doubt on the thoroughness of the Special Committee's investigation.

254. The thoroughness of the Special Committee's investigation is also placed in doubt by its admission that it limited its document review to the period

beginning July 29, 2017, failing to review documents generated between March 7, 2017 and July 28, 2017, when the warnings and alerts were first provided to Equifax and the Data Breach was taking place. There is also no mention in the report of the Special Committee reviewing external brokerage records of senior officers and directors.

255. Moreover, Defendant Hough is not independent or impartial because his son, Houston Hough, is an employee of Equifax, as acknowledged by the Company in SEC filings. Therefore, it would be impossible for Hough not to be biased or influenced by the fact that any finding against Equifax or any of the Individual Defendants could impact his son's position at Equifax and threaten his livelihood.

256. Since the Data Breach was publicly disclosed, Institutional Shareholder Services ("ISS"), a proxy advisory firm, recommended that Equifax shareholders vote against the re-election of several of the Individual Defendants, including Defendants Hough and Stock. As such, they both share a self-interest of exonerating the Individual Defendants and themselves to preserve their lucrative, prestigious positions at Equifax.

257. Moreover, a majority of the Board is neither independent nor disinterested for purposes of considering the Demands, but rather face a substantial

likelihood of liability for their actions and failures to act described herein. Accordingly, they would be unwilling to bring suit against each other.

XI. CAUSES OF ACTION

COUNT I

BREACH OF FIDUCIARY DUTY (AGAINST THE INDIVIDUAL DEFENDANTS)

258. The Individual Defendants owed and owe Equifax fiduciary obligations. By reason of their fiduciary relationships, the Individual Defendants owed and owe Equifax the highest obligation of loyalty, good faith, due care, oversight, and candor.

259. All of the Individual Defendants violated and breached their fiduciary duties of loyalty, good faith, due care, oversight, and candor.

260. Each of the Individual Defendants had actual or constructive knowledge that, among other things: (1) they and the Company failed to have reasonable and necessary risk oversight, information security, internal control monitoring, crisis management governance, and disclosure controls; (2) they and the Company failed to comply with applicable laws, regulations, industry standards and Equifax's Code of Ethics and Business Conduct; (3) they utterly disregarded safeguarding the critically sensitive and confidential information and data which they undertook to guard; (4) they and the Company failed to take adequate

measures to protect the Company's data systems; (5) they and the Company ignored numerous red flags, warnings and instructions to install the Apache patch; (6) they and the Company failed to maintain adequate monitoring systems to detect security breaches; and (7) they and the Company failed to develop an effective management crisis plan.

261. The Individual Defendants failed to comply with Equifax's Charter and its Code of Ethics and Business Conduct, with Georgia law, and with Federal law.

262. The Individual Defendants consciously caused or allowed Equifax to operate without requisite internal controls and, as a result, the Company regularly made false and misleading statements regarding its data protection systems.

263. The Individual Defendants consciously disregarded their oversight and monitoring responsibilities involving the Company.

264. The Individual Defendants' actions and failures to act were breaches of their fiduciary duties to Equifax and its shareholders and could not have been a good faith exercise of prudent business judgment to protect and promote the Company's corporate interests.

265. The Individual Defendants' actions and failures to act have subjected Equifax to material enterprise risk from enormous liability, damages, penalties and

fines in securities, consumer and financial institution class action litigation; numerous investigations, lawsuits and civil enforcement actions by regulators and government bodies; lost business and cancelled contracts; resource constraints; incremental IT and data security costs; legal, consulting, investigative, and other fees and expenses; severe and lasting damage to the Company brand, reputation, and competitive position; and loss of billions of dollars of market capitalization.

266. Per the Ponemon Institute, a pre-eminent research center dedicated to privacy, data protection and information security policy, in 2017 the average cost per stolen record in a data breach was $141.00. In Equifax's case, this equates to damages in excess of $20,000,000,000.

267. As a result of the misconduct alleged herein, the Individual Defendants are liable to the Company.

COUNT II

BREACH OF FIDUCIARY DUTY FOR INSIDER SELLING AND MISAPPROPRIATION OF INFORMATION (AGAINST GAMBLE, LOUGHRAN, PLODER AND BRANDBERG)

268. At the time of the stock sales detailed herein, Defendants Gamble, Loughran, Ploder and Brandberg knew of material non-public information concerning the Company's inadequate security measures and the Breach and sold Equifax common stock on the basis of such information.

269. Knowledge of the Company's inadequate security measures and the Breach was a proprietary asset belonging to the Company, which defendants Gamble, Loughran, Ploder and Brandberg used for their own benefit when they sold Equifax common stock.

270. Defendants Gamble, Loughran, Ploder and Brandberg's sales of Company common stock while in possession and control of material adverse non-public information was a breach of their fiduciary duties of loyalty and good faith.

271. Since the use of the Company's proprietary information for their own gain constitutes a breach of defendants Gamble, Loughran, Ploder and Brandberg's fiduciary duties, the Company is entitled to the imposition of a constructive trust on any profits defendants Gamble, Loughran, Ploder and Brandberg obtained thereby.

COUNT III

UNJUST ENRICHMENT
(AGAINST GAMBLE, LOUGHRAN, PLODER AND BRANDBERG)

272. Defendants Gamble, Loughran, Ploder and Brandberg were unjustly enriched by their receipt of proceeds from their illegal sales of Equifax common stock, as alleged herein, and it would be unconscionable to allow them to retain the benefits of their illegal conduct.

COUNT IV

UNJUST ENRICHMENT
(AGAINST THE EXECUTIVE DEFENDANTS)

273. Defendant Smith received and is to receive excessive and unwarranted compensation under the Retirement Agreement as alleged herein. Smith was and will be unjustly enriched by his receipt of compensation from the Retirement Agreement as alleged herein, and it would be unconscionable to allow him to retain or receive the excessive and unwarranted payments.

274. The Executive Defendants received excessive incentive-based compensation because their failure to expend the necessary funds to prevent the Breach caused Equifax's reported financial metrics to be inflated, which correspondingly inflated the Executive Defendants' compensation. The Executive Defendants were unjustly enriched by their receipt of this compensation, and it would be unconscionable to allow them to retain the excessive and unwarranted payments they have received.

COUNT V

VIOLATIONS OF SECTION 10(B) OF THE EXCHANGE ACT AND SEC RULE 10B-5
(AGAINST THE DIRECTOR DEFENDANTS)

275. In connection with Equifax's repurchase of shares, the Director Defendants disseminated and/or approved materially false and/or misleading

statements about Equifax, which they knew, or recklessly disregarded, were false or misleading and were intended to deceive, manipulate, or defraud. Those false or misleading statements and the Director Defendants' course of conduct were designed to artificially-inflate the price of the Company's common stock.

276. At the same time that Equifax's stock price was inflated due to the Director Defendants' false or misleading statements, the Director Defendants caused the Company to repurchase millions of shares of common stock. The Director Defendants engaged in a scheme to defraud Equifax by causing the Company to spend over $77 million repurchasing shares of Equifax stock at artificially-inflated prices.

277. The Director Defendants violated Section 10(b) of the Securities Exchange Act of 1934 (the "Exchange Act") and SEC Rule 10b-5 in that they (a) employed devices, schemes, and artifices to defraud; (b) made untrue statements of material facts or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and/or (c) engaged in acts, practices, and a course of business that operated as a fraud or deceit upon Equifax in connection with the Company's purchases of Equifax stock.

278. The Director Defendants, individually and in concert, directly and indirectly, by the use of means or instrumentalities of interstate commerce or the United States mails, engaged and participated in a continuous course of conduct that operated as a fraud and deceit upon the Company; made various false or misleading statements of material facts and omitted material facts necessary in order to make the statements, in light of the circumstances under which they were made, not misleading; made the above statements intentionally or with a severely reckless disregard for the truth; and employed devices and artifices to defraud in connection with the purchase and sale of Equifax stock, which were intended to, and did, (i) deceive Equifax regarding, among other things, the Company's grossly deficient data security, the Company's internal controls and compensation practices, and the Company's financial statements; (ii) artificially inflate and maintain the market price of Equifax stock; and (iii) cause Equifax to purchase the Company's stock at artificially-inflated prices, and suffer losses when the true facts became known.

279. The Director Defendants were the directors of the Company, and were, therefore, directly responsible, and are liable for all materially false or misleading statements alleged above.

280. The misstatements and omissions of material facts set forth herein were either known to the Director Defendants or were so obvious that the Director Defendants should have been aware of them. The Director Defendants also had a duty to disclose new information that came to their attention and rendered their prior statements to the market materially false or misleading.

281. The Director Defendants' false or misleading statements and omissions were made in connection with the purchase or sale of the Company's stock, both by the Company itself and by defendants Gamble, Loughran, and Ploder.

282. As a result of the Director Defendants' misconduct, Equifax has and will suffer damages in that it paid artificially inflated prices when purchasing Equifax common stock and suffered losses when the previously undisclosed facts relating to the Breach and the Company's cybersecurity deficiencies were disclosed. Equifax would not have purchased these securities at the prices it paid, but for the artificial inflation in the Company's stock price caused by the Director Defendants' false or misleading statements.

283. As a direct and proximate result of the Director Defendants' wrongful conduct, the Company suffered damages in connection with its purchases of

Equifax stock. By reason of such conduct, the Director Defendants are liable to the Company pursuant to Section 10(b) of the Exchange Act and SEC Rule 10b-5.

284. Lead Plaintiffs brought this claim within two years of their discovery of the facts constituting the violations and within five years of the violations.

COUNT VI

VIOLATIONS OF SECTION 29(B) OF THE EXCHANGE ACT (AGAINST THE INDIVIDUAL DEFENDANTS)

285. The Individual Defendants each received incentive pay, compensation, and fees, including stock awards and options, while engaging in conduct that violates Section 10(b) of the Exchange Act. The Individual Defendants' incentive compensation and fees should be rescinded under Section 29 of the Exchange Act because the Individual Defendants violated Section 10(b) by making untrue statements of material facts or omitting material facts necessary in order to make the statements made, in light of the circumstances, not misleading as described herein. All of the payments the Individual Defendants received are therefore voidable by Equifax under Section 29(b) of the Exchange Act.

286. Equifax is in privity with each of the Individual Defendants with respect to the incentive compensation and fees provided by Equifax to the Individual Defendants. The Individual Defendants have engaged in prohibited conduct in violation of the securities laws as alleged herein.

287. Equifax has been severely injured by the misconduct of the Individual Defendants. Accordingly, Equifax is entitled to damages, such as rescission of the incentives, compensation, and fees granted to the Individual Defendants.

COUNT VII

VIOLATIONS OF SECTION 14 OF THE EXCHANGE ACT AND RULE 14A-9 (AGAINST THE DIRECTOR DEFENDANTS)

288. This claim is based solely on negligence, not on any allegation of reckless or knowing conduct by or on behalf of the Director Defendants. Plaintiffs specifically disclaim any allegation or reliance upon any allegation or reference to any allegation of fraud, scienter, or recklessness with regard to this claim.

289. SEC Rule 14a-9 (17 C.F.R. § 240.14a-9), promulgated under Section 14(a) of the Exchange Act, provides:

> No solicitation subject to this regulation shall be made by means of any proxy statement form of proxy, notice of meeting or other communication, written or oral, containing any statement which, at the time and in the light of the circumstances under which it is made, is false or misleading with respect to any material fact, or which omits to state any material fact necessary in order to make the statements therein not false or misleading or necessary to correct any statement in any earlier communication with respect to the solicitation of a proxy for the same meeting or subject matter which has become false or misleading.

290. The Director Defendants negligently issued, caused to be issued, and participated in the issuance of materially misleading written statements to

stockholders that were contained in the 2014, 2015and 2016 Proxy Statements. The 2014, 2015 and 2016 Proxy Statements contained proposals to Equifax's stockholders urging them to re-elect the members of the Board and approve executive compensation. The Proxy Statements, however, misstated or failed to disclose material deficiencies in Equifax's internal and disclosure controls that were known to the Board when the Proxy Statements were filed; and that Equifax faced significant financial and reputational harm when the truth would inevitably unfold.

291. Equifax's 2017 Proxy Statement, like its 2014, 2015 and 2016 Proxy Statements, represented that that the Company has "a **rigorous enterprise-wide risk management program** ('ERM') targeting controls over operational, financial, legal/regulatory compliance, reputational, technology, privacy, **data security**, strategic and other risks that could adversely affect our business. The program also includes **crisis management** and business continuity planning." The Company added that: "Our CEO and senior leadership team receive comprehensive periodic reports on the most significant risks from the director of our internal audit department." (Emphasis added).

292. In truth, however, as subsequent events demonstrated, data security was not a "huge priority" for Equifax, the Individual Defendants did not establish a

"rigorous" enterprise risk or crisis management program," and, as such, caused Equifax to breach its obligations as a "trusted steward" for consumers and businesses.

293. Moreover, contrary to the representation in Equifax's 2017 Proxy Statement, under the heading "Board Expertise and Skills," that "Our Board is composed of experienced leaders with the right skill and business experience to provide sound judgment, critical viewpoints and guidance," and contrary to similar representations in its 2014, 2015 and 2016 Proxy Statements, the members of the Board's Technology Committee, whose responsibilities include providing "guidance on technology as it may pertain to, among other things, . . . security concerns" and overseeing "the execution of technology strategies formulated by management and technology risks," did not have data risk management expertise or experience or "the right skill and business experience to provide sound judgment, critical viewpoints and guidance."

294. By reason of the conduct alleged in this Complaint, the Director Defendants violated Section 14(a) of the Exchange Act and SEC Rule 14a-9. As a direct and proximate result of the Director Defendants' wrongful conduct, Equifax misled or deceived its stockholders by making misleading statements that were an

essential link in stockholders heeding Equifax's recommendation to re-elect the current Board and approve certain executive compensation.

295. The misleading information contained in the 2014, 2015 and 2016 Proxy Statements was material to Equifax's stockholders in determining whether or not to elect the Director Defendants and approve certain executive compensation. This information was also material to the integrity of the directors who were proposed for election to the Board. The proxy solicitation process in connection with the Proxy Statements was an essential link in the reelection of nominees to the Board and the approval of the executive compensation plan.

296. Lead Plaintiffs, on behalf of Equifax, seek relief for damages inflicted upon the Company based on the misleading Proxy Statements in connection with the improper re-election of the members of the Board and approval of executive compensation.

297. This action was timely commenced within three years of the date of each Proxy Statement and within one year from the time Lead Plaintiffs discovered or reasonably could have discovered the facts on which this claim is based.

COUNT VIII

CORPORATE WASTE
(AGAINST THE DIRECTOR DEFENDANTS)

298. The Director Defendants approved and paid Smith the excessive and unwarranted compensation under the Retirement Agreement and established the system and approved the amounts of incentive-based compensation for the Executive Defendants. In exchange for the excessive and unwarranted compensation, the Company received no consideration or consideration so disproportionately small as to lie beyond the range at which any reasonable person might be willing to trade.

299. As a direct and proximate result of the Director Defendants' waste of corporate assets, Equifax has sustained damages.

XII. PRAYER FOR RELIEF

WHEREFORE, Lead Plaintiffs request the following relief:

A. Declaring that Lead Plaintiffs may maintain this derivative action on behalf of Equifax and that Lead Plaintiffs are proper and adequate representatives of the Company;

B. Declaring that the Individual Defendants have breached their fiduciary duties to Equifax;

C. Awarding to Equifax from each of the Individual Defendants, jointly and severally, and from their Directors' and Officers' insurance policies, the amount of damages sustained by the Company as a result of their breaches of fiduciary duties, unjust enrichment, violations of securities laws, and waste of corporate assets;

D. Determining that Defendant Smith may not retain or receive the excessive and unwarranted compensation under his Retirement Agreement;

E. Ordering Gamble, Loughran, Ploder, and Brandberg to disgorge to the Company all proceeds derived from their sales of Equifax common stock alleged herein;

F. Ordering the Executive Defendants to disgorge the portion of their incentive-based and other compensation that was inflated due to lax data security policies;

G. Granting appropriate equitable relief or injunctive relief to remedy the Individual Defendants' breaches of fiduciary duties and other violations of law, including, but not limited to the institution of appropriate cybersecurity, corporate governance, risk oversight,

internal control monitoring, and supervision, crisis management governance, and disclosure controls;

H. Awarding to Lead Plaintiffs the costs and disbursements of the action, including reasonable attorneys' fees, accountants' and experts' fees, costs and expenses; and

I. Granting such other and further relief as the Court deems just and proper.

XIII. JURY DEMAND

300. Lead Plaintiffs demand a trial by jury of all issues so triable.

Dated: July 12, 2018

Respectfully submitted,

WEISSLAW LLP
Michael A. Rogovin
Georgia Bar No. 780075
476 Hardendorf Ave. NE
Atlanta, Georgia 30307
Telephone: (404) 692-7910
Facsimile: (404) 795-5778
mrogovin@weisslawllp.com

WEISSLAW LLP
By: */s/ Joseph H. Weiss*
Joseph H. Weiss (*pro hac vice*)
David C. Katz
Mark D. Smilow
Joshua M. Rubin (*pro hac vice*)
1500 Broadway, 16th Floor
New York, New York 10036
Telephone: (212) 682-3025
Facsimile: (212) 682-3010
jweiss@weisslawllp.com
msmilow@weisslawllp.com
jrubin@weisslawllp.com

Counsel for Lead Plaintiffs Nancy A.K. and John Weyl and Lead Derivative Counsel

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing was filed with this Court via its CM/ECF service, which will send notification of such filing to all counsel of record this 12th day of July, 2018.

/s/ Joseph H. Weiss